Attorney Docket No. 122.1569

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Kimitaka MURASHITA, et al.

Application No.: Group Art Unit:

Filed: November 4, 2003 Examiner:

For: BIOMETRIC AUTHENTICATION SYSTEM

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-170723

Filed: June 16, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: November 4, 2003 By: _____

H. J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月１６日

出願番号
Application Number: 特願２００３－１７０７２３

[ST. 10/C]: [ＪＰ２００３－１７０７２３]

出願人
Applicant(s): 富士通株式会社

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０５７８４６

【書類名】　特許願

【整理番号】　0350293

【提出日】　平成15年 6月16日

【あて先】　特許庁長官　太田　信一郎　殿

【国際特許分類】　G06F 15/00

G06K 17/00

G06K 19/00

【発明の名称】　認証端末装置、生体情報認証システム、及び生体情報取得システム

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　村下　君孝

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　新崎　卓

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鈴木　祥治

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】
　【識別番号】　100099759
　【弁理士】
　【氏名又は名称】　青木　篤
　【電話番号】　03-5470-1900
【選任した代理人】
　【識別番号】　100092624
　【弁理士】
　【氏名又は名称】　鶴田　準一
【選任した代理人】
　【識別番号】　100100871
　【弁理士】
　【氏名又は名称】　土屋　繁
【選任した代理人】
　【識別番号】　100082898
　【弁理士】
　【氏名又は名称】　西山　雅也
【手数料の表示】
　【予納台帳番号】　209382
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0305916
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証端末装置、生体情報認証システム、及び生体情報取得システム

【特許請求の範囲】

【請求項１】　本人に係る複数の生体情報を格納した生体情報保持部を備え、少なくとも一つの前記生体情報が、当該本人の認証に使用される端末装置。

【請求項２】　前記生体情報は、種類の異なる生体情報を含む請求項１に記載の端末装置。

【請求項３】　本人に係る複数の生体情報を格納した生体情報保持部と、

生体情報を取得する生体情報取得部と、

前記取得した生体情報と前記生体情報保持部に格納された生体情報に基づき前記本人認証を行う本人認証部と、

前記本人認証部で本人と認証された場合に、前記生体情報保持部から所定の生体情報を選択して出力する生体情報出力部と

を備える端末装置。

【請求項４】　前記生体情報保持部から選択された前記生体情報を、該生体情報に対応する特定のビット長からなる生体情報対応データを生成する生体情報対応データ生成部を備え、

該生成された生体情報対応データを前記生体情報送信部より送信する請求項３に記載の端末装置。

【請求項５】　本人にかかる複数の生体情報を格納する生体情報保持部と、少なくとも一つの前記生体情報を送信する生体情報送信部とを有する端末装置と、

生体情報を照合すべき辞書情報として保持する辞書情報保持部と、前記生体情報送信部から送信される前記生体情報と前記辞書情報保持部に格納されている辞書情報とに基づいて第１の本人認証を行う第１本人認証部を有する認証装置と

を備えた生体情報認証システム。

【請求項６】　前記端末装置は、生体情報を取得する生体情報取得部と、第２の本人認証を行う第２本人認証部とを備え、

前記取得された生体情報と前記生体情報保持部に格納された生体情報とを用いて第２の本人認証を行い、当該本人と認証された場合に、前記第１本人認証部において使用する生体情報を前記生体情報送信部より前記認証装置に送信する請求項５に記載の生体情報認証システム。

【請求項７】　前記認証装置は、前記端末装置から送信される前記生体情報に基づいて前記生体情報に対応する特定のビット長からなる生体情報対応データを生成する生体情報対応データ生成部を備え、

該生成された生体情報対応データにより前記辞書情報保持部に格納されている辞書情報を特定し、前記第１本人認証部において、該特定された辞書情報と前記送信された生体情報とに基づいて本人認証を行う請求項５又は６に記載の生体情報認証システム。

【請求項８】　前記認証装置は、第１本人認証部で使用する生体情報のフォーマット情報を格納する変換情報保持部を備え、

前記端末装置は、前記生体情報保持部に格納された前記生体情報のフォーマットを変換する生体情報変換部を備え、

前記生体情報変換部は、前記変換情報保持部から送信された前記フォーマット情報を用いて前記生体情報のフォーマットを変換し、該フォーマット変換された前記生体情報を前記認証装置に送信する請求項５～７のいずれか一項に記載の生体情報認証システム。

【請求項９】　本人に係る複数の生体情報を格納する生体情報保持部と、前記生体情報保持部に格納された複数の生体情報から選択された前記生体情報に対応する特定のビット長からなる生体情報対応データを生成する第１生体情報対応データ生成部と、該生成された第１生体情報対応データを送信する生体情報対応データ送信部とを有する端末装置と、

生体情報を照合すべき辞書情報として保持する辞書情報保持部と、前記辞書情報に対応する特定のビット長からなる生体情報対応データを生成する第２生体情報対応データ生成部と、送信された前記第１生体情報対応データ及び第２生体情報対応データに基づいて第１の本人認証を行う第１本人認証部と

を有する認証装置とを備えた生体情報認証システム。

【請求項１０】　本人に係る複数の生体情報を格納する生体情報保持部を有する端末装置と、

前記端末装置から送信される前記生体情報に基づいて本人認証を行う認証装置と、

前記生体情報を取得するための生体情報取得部と該生体情報を暗号鍵により暗号化する暗号化部と復号鍵を格納する復号鍵格納部とを有する生体情報取得装置とを備え、

前記生体情報取得部により取得された前記本人に係る生体情報は、前記暗号化部で暗号化して前記端末装置の前記生体情報保持部に格納され、前記端末装置に格納された前記暗号化された生体情報が前記認証装置に送信されたときに、該認証装置において前記生体情報取得装置の前記復号鍵格納部に格納された前記復号鍵を使用して前記暗号化された生体情報を復号する生体情報取得システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証端末装置及び個人認証システムに関し、特に生体情報を送信する認証端末装置及び生体情報認証システムに関する。

【０００２】

【従来の技術】

重要な施設等への入室や、ネットワーク上でのサービスを受けるためのアクセスに際して、従来から、ＩＤとパスワード、又は磁気カードやＩＣカード等を用いる本人認証が行われている。ＩＤとパスワードを用いる本人認証システムは、ユーザに割り振られたユーザ固有の番号（ＩＤ）と、システムあるいはユーザが設定したパスワードとの組がシステム上に格納され、ユーザはサービスを利用する際、ＩＤとパスワードを入力し、システム上で格納しているユーザのＩＤとパスワードとを比較し、一致すればユーザ本人であると見なす。ＩＣカードを用いる本人認証システムは、正規ユーザにＩＣカードを提供し、システムにアクセスする際にカードリーダにカードを読み込ませることでユーザ本人であることを認証する。

【０００３】

ＩＤとパスワードは，知っていれば誰でも本人になりすますことができるという欠点がある。これらは無形の情報であるため、パスワードが第三者に漏洩したことを知るのは難しい。また、ＩＣカードは、紛失や盗難があると容易に分るが、そもそも紛失や盗難される機会が多く、ユーザが紛失や盗難に気付くまでの間に第三者によって不正に利用されるという恐れがある。このように、ＩＤとパスワードは「知っている人」を正規ユーザとみなし、ＩＣカードは「所持している人」を正規ユーザとみなして本人認証しているので、本人認証システムとしては問題がある。

【０００４】

それに対して、確実に本人を認証する方法として生体情報認証がある。生体情報認証では、ユーザ本人を特定することができる生体情報をユーザの識別子として利用する。ユーザの生体情報は偽造困難であり、同じ情報を持つ人がいない（万人不等）、ユーザの成長など経年変化で変動しない（生涯不変）の特徴を持つ。具体的には指紋、声紋、掌紋、掌形、静脈、虹彩、網膜などが使用される。現在では、さらに音声や署名なども生体情報として本人認証に用いられている。生体情報認証は、パスワードやＩＣカードなどと異なり、他人がなりすますことができない本人認証手段として注目されている。

【０００５】

生体情報認証システムの従来例を図１４に、従来のフローチャートを図１５に示す。図１４には、一例として、指紋認証システムと虹彩認証システムを示した。

【０００６】

指紋認証システムは、指紋認証サーバ９１とクライアント端末９５及び９７とからなる。指紋認証サーバ９１は、指紋データ辞書部９１１とデータ照合部９１２を備え、クライアント端末９５及び９７は、それぞれ指紋センサ９５１及び９７１を備える。ここでは、クライアント端末９７は、指紋センサと虹彩センサを備えて、指紋認証システム及び虹彩認証システムの両方に対応できるようになっている。指紋認証サーバ９１の辞書部９１１には、予めユーザから取得又は提供

された指紋情報データあるいは該指紋情報から抽出した特徴点データを格納しておく。これらのデータはデータ照合用の辞書データとなる。

【０００７】

次に、図１５のフローに従って指紋認証のプロセスを説明する。

ステップＳ１０では、ユーザはクライアント端末９５又は９７に設置された指紋取得用センサに指紋を入力する。

【０００８】

ステップＳ２０では、指紋データはサーバ９１に送信される。

次いで、ステップＳ３０で、送信された指紋データは、辞書部９１１から出力される辞書データと比較される。特徴点の一致数が予め定めた閾値以上であれば同一の指紋情報とみなしてユーザ本人であると認証し、すべての辞書データと比較した結果、一致数が閾値以下であれば認証されない。

【０００９】

虹彩認証システムも、同様に、虹彩認証サーバ９２とクライアント端末９６及び９７とからなる。虹彩認証サーバ９２は、虹彩データ辞書部９２１とデータ照合部９２２を備え、クライアント端末９６及び９７は、それぞれ虹彩センサ９６２及び９７２を備える。虹彩認証システムの認証動作も、指紋認証システムと同様に行われる。

このような従来の認証システムにあっては、虹彩認証システムと指紋認証システムは、各システムに対応するセンサを個々に必要とし、一つのセンサを備える端末は、そのセンサに対応するシステムにしか対応することができない。両システムに対応しようとすると、端末９７のように、２つのセンサを揃える必要があった。

【００１０】

また、生体情報による認証システムの例として次のようなものがある（特許文献１参照）。

【００１１】

特許文献１によれば、まず、登録端末側で採取した生体情報をユーザが所持する個人情報蓄積媒体に格納された暗号化鍵で暗号化してサーバ上に保存しておく

。次に、サーバに対してユーザの認証要求があると、該暗号化済み生体情報を認証端末に送信する。認証端末においては、ユーザの個人情報蓄積媒体に格納された暗号化鍵でサーバから送信された暗号化済み生体情報を復号する。認証端末では、ユーザが認証端末に具備されているセンサで入力した生体情報と、前記復号した生体情報とを照合してユーザであるか否かを認証する。

【００１２】

【特許文献１】

特開２００２－２９７５５１号公報

【００１３】

【発明が解決しようとする課題】

このような従来の生体情報認証システムには、以下の課題がある。

（１）複数の生体情報認証システムが乱立しており統一されていない。

【００１４】

従来例として、指紋認証システムと虹彩認証システムを示したが、生体情報には指紋、声紋、掌紋、掌形、静脈、虹彩、網膜、音声、署名などが用いられている。それぞれ、認証精度が高い、簡単に収集できる、ユーザの心理的抵抗が低いなど、長所・短所があり、どの生体情報が最適とは一概に言えない。

【００１５】

システム毎の仕様（セキュリティ要求性能、ユーザ数など）によって、個別の生体情報をそれぞれのシステムが独自に使用している。ＩＤ・パスワードはキーボード、ＩＣカードはＩＣカードリーダがあればよいが、生体情報認証では生体情報ごとに個別の入力装置（センサ）が必要になる。また、同じ生体情報を用いていても、システムが要求する生体情報のフォーマット（解像度、画素数、階調数など）が異なっていれば、やはりシステムごとに個別のセンサが必要になる。

【００１６】

このように現在では、使用する生体情報の種類やフォーマットが統一されておらずシステムごとに異なるため、システム構築をする際、システムごとにセンサを端末に設置する必要がある。これはシステム全体のコストアップの要因となる。

【００１７】

（２）ユーザ数が多くなるとターンアラウンドタイム（認証処理時間）が長くなる。

生体情報認証では、通常、ＩＤのようなユーザ識別子を使用せず、生体情報だけでユーザ認証を行う。システムに複数ユーザが登録されている場合、システムは登録ユーザ一人一人に対して照合を行う（１：Ｎ照合）。例えばシステムに１０００人のユーザが登録されている場合、ユーザ認証では最大１０００回の認証処理を実行する。１回の照合処理が１００ｍｍ秒程度の高速処理であっても、１０００人のユーザが登録されているシステムでは最大１００秒の処理時間がかかることになる。このように、レスポンスタイムは、ユーザ数に比例して増加する。

【００１８】

（３）生体情報をサーバ側に送付する必要があり、盗聴などによる漏洩の危険がある。

【００１９】

生体情報は偽造は困難であるが、第三者に盗まれる恐れがある。例えば指紋の場合、指紋センサから入力された画像データをサーバ側に送信するのであるが、このデータを盗聴された場合、第三者が不正に流用してしまう恐れがある。指紋は生涯不変であるため、一度流出した指紋画像を取り消すことはできず、以後、その指紋は本人認証に使えなくなってしまう。

【００２０】

通信経路を暗号化するなどの方策が考えられるが、暗号化も万全ではなく解読の恐れがある。ＩＤ・パスワード認証では、このような課題を解決する手段として、パスワードそのものを送るのでなく、パスワードから生成されるチャレンジデータを送るチャレンジコード認証を行っている。

【００２１】

チャレンジコード認証は、サーバから送信される可変長のパスワードを、クライアント側で特定の処理を行って変換して一定長の文字列を生成し、それをサーバに転送する。サーバ上でも同様のチャレンジコード生成を行い、チャレンジコ

ードが一致するかどうかを検証するものである。パスワード自体は送付しないため、第三者にパスワードが流出することはなく、チャレンジコード生成も、パラメータを毎回変え、それをサーバ側とユーザ側とで同期させることで、毎回異なるチャレンジデータを送付することができる。チャレンジデータ生成の具体例としては、ＲＦＣ１３２１（Network Working Group Request for Comment: 1321）で規定されているＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　５）が有名である。

【００２２】

ＩＤ・パスワード認証におけるチャレンジデータは、サーバ側とユーザ側とで元となるデータ（パスワード）が同一であるため、両者の結果が一致するが、指紋などの生体情報は、ユーザ側でセンサから入力されるデータは毎回微妙に異なるデータであるため、ユーザ側とサーバ側とでチャレンジデータを生成しても一致することはない。そのため、生体情報を用いたチャレンジコード認証はできなかった。

【００２３】

（４）生体情報取得用のセンサは高価で、システム運営者やユーザのコスト負担が重い。

【００２４】

生体情報を取得するためのセンサは高価である。システム運営者がセンサを購入する場合、ユーザの利便性を確保するためには、ユーザ数に応じて多くのセンサを設置する必要がある。利用するユーザにセンサのコストを負担させる方法もあるが、これはユーザがシステムを利用する敷居となり、システムの普及を遅らせる可能性がある。

【００２５】

特許文献１に記載の認証システムは、異なる端末間においても安全確実に認証可能なシステムを得ることを目的とするもので、複数の認証システムに対応することを課題とするものではない。

【００２６】

本発明は、前記問題点に鑑み、複数の生体情報認証に対応できる端末及びシス

テムを提供することにより、従来システムでは解決できない前記（１）～（４）の課題を解決することを目的とする。

【００２７】

【課題を解決するための手段】

本発明は、前記課題を解決するために、端末装置に生体情報保持部を設け、そこに本人に係る複数の生体情報を格納した。この複数の生体情報は、異種の生体情報とすることができる。本発明の端末装置は、本人に係る複数の生体情報を備えることにより、複数の認証システムに対応できるものである。

また、本発明は、認証装置と端末装置からなる生体情報認証システムであって、端末装置には本人に係る複数の生体情報を格納する生体情報保持部を備え、生体情報保持部に格納された複数の生体情報から選択して、端末装置から認証装置に対して生体情報を送信して認証装置において本人認証を可能とする生体情報認証システムを提供する。

さらに、前記端末装置には、生体情報を取得する生体情報取得部と、本人認証を行う第２本人認証部とを備え、取得された生体情報と生体情報保持部に格納された生体情報とを用いて第２の本人認証を行い、本人と認証された場合に認証装置の第１本人認証において使用する生体情報を認証装置に送信することができる。

さらに、本人認証に用いる生体情報は、端末装置の生体情報保持部に保持されているものであるから、この生体情報に基づいて生体情報に対応する特定のビット長からなる生体情報対応データを生成して、この生体情報対応データを利用することもできる。

さらに、本発明は、認証装置及び端末装置に加えて、本人認証に用いる生体情報を取得する生体情報取得装置を含む生体情報取得システムを提供する。このシステムでは、端末装置の生体情報保持部に生体情報を格納するときに、生体情報取得装置を利用する。生体情報取得装置では、取得される生体情報は暗号化されて、端末装置の生体情報保持部に格納される。生体情報を本人認証に使用するために、端末装置から認証装置にこの生体情報が送信されると、認証装置は、生体情報取得装置から復号鍵を得て、受信した暗号化生体情報を復号する。このよう

にすると、本人認証に使用する生体情報の取得に対して認証装置に課金することが可能となる。

【００２８】

【発明の実施の形態】

図面を参考にして、以下に本発明の実施の形態を説明する。各図を通して同一のものには、同一の符号を付した。

まず、図１を参照して、本発明による端末の、各実施形態に共通する基本形を説明する。図１には、本発明による端末１０を示す。端末１０は、生体情報認証システムの認証装置（サーバ）（図示せず）に要求された生体情報Ｂ１を出力する機能を有する。端末１０は、生体情報を出力する機能をもつどのようなものであってもよいが、例えば携帯電話、ＰＤＡ（personal digital assistant）、ＩＣカード等であれば、携帯に便利である。

本発明による端末１０は、予め複数の生体情報を格納した生体情報保持部１と、端末装置種類の所有者の生体情報を取得するセンサ２と、所有者の生体情報認証を行う所有者認証部３と、生体情報保持部１内の生体情報を出力する生体情報出力部４を有する。生体情報保持部１に格納された生体情報は、生体情報認証のために用いられるものであって、具体的には指紋、声紋、掌紋、静脈、虹彩、網膜、サイン、顔等に関するデータ及びこれらから抽出された特徴点データである。

【００２９】

ここで、生体情報を取得するセンサ２が指紋センサであり、図示しない認証装置が要求する生体情報が虹彩情報Ｂ１であるとする。従来の端末であれば、ＣＣＤカメラのような虹彩情報を取得できるセンサが端末に備わっていなければ、虹彩情報を送信することはできなかった。しかしながら、本発明による端末２０であれば、虹彩センサを備えていなくても、虹彩情報Ｂ１を送信することができる。すなわち、指紋センサ２により、本人の生体情報である指紋情報Ｂ２１を入力する。入力された指紋情報２１は、認証部３に送られる。同時に、生体情報保持部１に格納された生体情報のうち指紋情報Ｂ２が認証部３に入力される。認証部３では両者が照合され、所有者であることが認証されると、認証装置が要求する

虹彩情報Ｂ１が生体情報保持部１から選択され、出力部４を介して認証装置に出力される。

【００３０】

このように、本発明による端末は、複数種類の生体情報を予め格納しておくことができるので、どのような生体情報認証システムに対しても適用可能である。ここでは、認証装置が要求する情報は虹彩情報Ｂ１であり、端末の生体情報センサは指紋情報Ｂ２を入力するものを例としたが、もちろんこれはあくまで説明のための１例である。

なお、基本形として、端末１にセンサ２及び認証部３を配置して所有者認証を行うものを示したが、センサ２及び認証部３は必ず端末１に備えていなければならないというものでもない。センサ２及び認証部３は、端末１とは別の装置に配置されていてもよい。

【００３１】

（第１実施例）

図２に示すように、本実施例のユーザ認証システムは、ユーザ認証装置又はサーバ１００と端末装置２００とからなる。通常、端末装置２００は多数存在し、ユーザ認証装置も一つとは限らない。端末装置２００は、パーソナルコンピュータでもよいし、携帯電話やＰＤＡ等の携帯情報端末あるいはＩＣカードでもよい。

【００３２】

ユーザ認証装置１００は、端末２００に対して生体情報の送信を要求する生体情報要求部１０１と、ユーザを生体情報認証するために必要な生体情報である辞書データを格納した辞書情報保持部１０２と、ユーザ認証を行うユーザ認証部１０３とを有する。

【００３３】

一方、端末装置２００は、予め複数の生体情報を格納した生体情報保持部２０１と、端末装置の所有者の生体情報を取得するセンサ２０２と、所有者の生体情報認証を行う所有者認証部２０３と、生体情報保持部２０１内の生体情報を出力する生体情報送信部２０４とを有する。生体情報保持部２０１には、ユーザ本人

を認証するための複数の生体情報が予め格納されている。すなわち、具体的には指紋、声紋、掌紋、静脈、虹彩、網膜、サイン、顔等から得られる情報である。

【００３４】

本実施例では、ユーザ認証装置の認証は虹彩情報による認証であり、端末の所有者認証は指紋情報による。ただし、これはあくまで説明のための一例であり、ユーザ認証装置において本人認証のために用いられる生体情報は、虹彩情報に限らずどのような生体情報であってもよく、端末に設ける生体情報センサも指紋センサに限定されるものではない。また、ユーザ認証装置における本人認証と端末における所有者認証とで、異なる生体情報を使用する必要もない。ただし、端末が、携帯電話やＰＤＡ等の携帯情報端末又はＩＣカードであれば、端末に設けられるセンサは、指紋センサのような小型で認証精度が高いセンサが望ましい。

【００３５】

次に、図２～４を参照して、本実施例のシステムの動作フローを説明する。

まず、ステップＳ１で、生体情報要求部１０２は端末装置２００に対して虹彩情報Ｂ１の出力を要求する生体情報要求信号ＲＢを送る。

【００３６】

ステップ２では、ユーザは、例えば表示装置（図示せず）に表示されたユーザ認証装置１００からの生体情報要求信号ＲＢを受けて、端末装置２００のセンサ２０２に生体情報を入力する。すなわち、ユーザは指紋センサであるセンサ２０２に登録指紋を有する指を押当てる。センサ２０２はユーザの指紋を読み取って指紋情報Ｂ２１を所有者認証部２０３に送る。

【００３７】

これに対して、ステップＳ３では、生体情報保持部２０１に保持されている所有者の指紋情報Ｂ２を所有者認証部２０３に送る。

【００３８】

ステップＳ４では、所有者認証部２０３において、センサが取得した指紋情報Ｂ１と、生体情報保持部２０１からの指紋情報Ｂ２とを比較して、例えば、特徴点データに変換して比較して、所有者認証を行う。認証結果がＯＫすなわち、ユーザが入力した指紋データの特徴点と生体情報保持部２０１に保持されている指

紋データの特徴点の一致数が予め定めた閾値以上であれば、認証結果は生体情報送信部２０４に出力される。

【００３９】

次に、ステップＳ５で、生体情報送信部２０４は、ユーザ認証装置１００が要求している生体情報である虹彩情報Ｂ１を生体情報保持部２０１より選択してユーザ認証装置１００に送信する。

【００４０】

ステップＳ６では、ユーザ認証装置１００の生体情報要求部１０２は、受信した生体情報Ｂ１がユーザ認証装置が要求した情報であるかどうかを確かめる。もし受信した情報が虹彩情報Ｂ１でないときには、再度虹彩情報の送信を要求する（ステップＳ１）。受信した情報が虹彩情報Ｂ１であれば、ユーザ認証部１０３へ送られる。

【００４１】

ステップＳ７では、辞書情報保持部１０１からユーザ認証部１０３へ認証照合のために虹彩情報Ｂが送られる。

【００４２】

ステップ８では、ユーザ認証部で受信した虹彩情報Ｂ１と辞書情報保持部１０１からの虹彩情報Ｂとを、例えば、特徴点データに変換して比較して照合し、正規ユーザであるかどうか認証する。正規ユーザと認証されれば、サービスが開始される。照合した結果前記の閾値以下であれば、ステップ９に進む。

【００４３】

ステップ９では、すべての辞書データと照合が済んだかどうかを判定し、すべて終了していれば、認証ＮＧとなり、認証は認められない。照合すべき辞書データが残っていると、ステップ７に戻って、次の虹彩情報Ｂとの照合を行う。

【００４４】

本実施例では、ユーザ認証装置１００による認証は虹彩認証として説明したが、その他の掌形認証や静脈認証、指紋認証などが行われる場合でも、これらの認証装置が要求する生体情報を予め取得して端末装置２００の生体情報保持部２０１内に格納しておけば、認証装置の要求に応答して必要な生体情報を送信するこ

とができる。

【００４５】

このように、端末に配置されているセンサでは入力できない生体情報が必要な場合であっても、ユーザ側の端末には、新たな生体情報取得用のセンサなどの追加の設備を設置する必要はない。同じ１台の端末でしかもユーザが入力する生体情報は同一のもので、多数のユーザ認証に利用することができる。

【００４６】

ユーザの端末への生体情報の取得は、ユーザがユーザ認証を必要とするサービスの申し込みをする際に、申込先（例えば店舗）で取得するようにできる。このようにすれば、生体情報を取得するためのセンサは、ユーザが実際にサービスを利用する端末装置に設置する必要はなく、サービス申し込みを受け付ける店舗にのみ設置しておけばよい。

【００４７】

（第２実施例）

従来の端末装置から送られる生体情報は、本人のものであっても毎回センサから入力されるものであるから、少しずつ異なる生体情報である。しかし、本発明による端末装置からユーザ認証装置に送信される生体情報は、生体情報保持部２０１に格納されているものであるから、常に同一のデータである。したがって、原理的には、この生体情報をそのままユーザＩＤのように使用することが考えられる。ただし、生体情報そのままでは、情報量が大きく冗長度も高い。

【００４８】

第２実施例では、ＩＤ認証で使用されているようなチャレンジデータを生成して、これを辞書データを特定するデータとして利用する。すなわち、第２の実施例は、ユーザ認証装置において、受信した生体情報をもとにチャレンジデータを生成し、このチャレンジデータをユーザを特定する識別子として用いる。

【００４９】

そのために、図５に示すように、ユーザ認証装置１１０は第１の実施例の生体情報要求部１０１と辞書情報保持部１０２との間に、チャレンジデータ生成部１１１とユーザ特定部１１２とを有する。端末装置２００は第１の実施例と同一の

ものである。

【００５０】

チャレンジデータ生成部１１３は端末装置２００から受信した生体情報Ｂ１を用いてチャレンジデータＣ０を生成する。チャレンジデータの具体的生成方法としては、ＲＦＣ１３２１で規定されているＭＤ５などが考えられる。ＭＤ５は可変長の入力データに対して１２８ビットの固定長データを出力する一方向ハッシュ関数である。これにより１２８ビットのユーザＩＤを生成することができる。辞書情報保持部の辞書データは、このチャレンジデータＣ０によってデータを特定できるような形態、例えばチャレンジデータをアドレスとするような形態で格納されている。ユーザ特定部１１２は、チャレンジデータ生成部１１１が生成したチャレンジデータＣ０を受けてユーザを特定し、該ユーザの辞書データＢ１の出力を辞書データ保持部１０１に要求する。辞書データ保持部１０１はユーザ認証部１０３に特定されたユーザの生体情報Ｂ１を送信し、ユーザ認証部１０３は特定されたユーザの辞書データＢ１と端末装置より受信した生体情報Ｂ１とを用いて照合し、ユーザ認証を行う。なお、ここでは説明を簡単にするために、照合される辞書データＢ１と端末装置より受信した生体情報を同じＢ１で示したが、生体情報保持部２０１に格納され送信される生体情報と、辞書情報保持部１０１に格納されている情報とが全く同一のデータである必要はない。

【００５１】

第１実施例の動作フローで説明したように、通常、生体情報認証では、ユーザ認証装置内に登録されているユーザの辞書データを順次認証し、一致するユーザがいるかどうか判別する（１：Ｎ認証）。このような１：Ｎ認証では、例えば１０００人のユーザが登録されていた場合、最大１０００回の認証処理を要する。１回の認証処理時間が１００ｍｓ程度の短時間であっても、１０００回認証すれば１００秒にもなる。登録ユーザ数が増えれば増えるほどユーザ認証装置がユーザ認証にかかる時間（ターンアラウンドタイム）は遅くなり、レスポンスが低下する。本実施例では、チャレンジデータにより辞書データを特定することにより、照合すべき生体情報を一つに絞ることができる。したがって、１回の認証（１：１認証）で正規ユーザかどうか判定できるため、登録ユーザ数に関係なく、常

に一定の短いターンアラウンドタイムで認証が実現できる。

【００５２】

（第３実施例）

第２実施例のように、チャレンジデータを生成する場合、チャレンジデータ生成部が出力するチャレンジデータは、入力データである生体情報に比べて十分小さな値となっている。そのため、異なる生体情報であっても、同一のチャレンジデータが生成（ハッシュ値の衝突が発生）される可能性がある。この場合、チャレンジデータにより生体情報を特定することはできない。

【００５３】

また、システムには、本発明による端末装置が備えられるだけではなく、従来型の端末装置が混在する場合もある。従来型端末装置は、ユーザ認証装置が要求する生体情報を取得するためのセンサを具備し、送信を要求される毎に該センサにより生体情報を取得するために、ユーザ認証装置に送信される生体情報は毎回異なる。そのため、異なる生体情報に基づいてチャレンジデータを生成しても、毎回異なるデータが生成され、ユーザを特定するために使用できない。

【００５４】

第３実施例では、このような課題を解決するために、ユーザ認証装置において、受信した生体情報からチャレンジデータを生成してユーザを特定して認証する処理と、登録されている全ユーザと順次照合した結果認証する処理との両方が可能となるように構成する。

【００５５】

図６に記載のように、本実施例では、ユーザ側において、本発明の端末装置２００と従来型の端末装置２１０とが混在する。従来型の端末装置２１０は、ユーザ認証装置１１１が要求する生体情報（虹彩情報Ｂ１１）を入力するセンサ（例えばＣＣＤカメラ）２１１を備え、ユーザ認証装置の要求を受けて、生体情報送信部２１２から、センサ２１１によって得られた虹彩情報Ｂ１１を送信するものである。ユーザ認証装置１１１には、第２実施例に示したものにさらに全ユーザ照合部１１３が付加されている。

【００５６】

ユーザ認証装置１１１では、まず、受信した生体情報をもとにチャレンジデータを生成する。生成されたチャレンジデータに基づいてユーザを特定できれば、該ユーザの虹彩情報である辞書データを用いてユーザ認証部１０３で認証を行う。ユーザの使用する端末装置が本発明の端末装置２００であった場合、生体情報Ｂ１からチャレンジデータＣ０を生成することができるから、第２実施例と同様に辞書データを特定して照合し、通常１回の認証処理で認証結果が得られる。

【００５７】

しかし、ユーザ側の端末装置が従来の端末装置２１０であれば、ユーザが同一人であっても送信された虹彩情報Ｂ１１は毎回異なり、生成されるチャレンジデータも異なるから、チャレンジデータによる認証はＮＧとなる。したがって、全ユーザ照合部１１３によって、ユーザ認証装置に登録されている全ユーザの辞書データＢを用いて送信された虹彩情報Ｂ１１のユーザ認証を行う。なお、全ユーザ照合部１１３の機能は、ユーザ認証部１０３によっても実現できる。

【００５８】

使用された端末装置が本発明による端末装置２００であり、虹彩情報Ｂ１が送信された場合でも、先に説明したように、ユーザ認証部１０３による認証がＮＧとなる場合もあり得る。この場合も、全ユーザ照合部１１３による照合に切替わることになる。

【００５９】

また、ユーザ認証装置に送られる生体情報が端末２００からのものか、端末２１０からのものかが判別できれば、端末の種類によってユーザ認証の方法を異ならせるようにしてもよい。すなわち、端末２００又は端末２１０の種類を判別できる信号を生体情報信号とともにユーザ認証装置に送り、端末２００から送られた生体情報信号Ｂ１は、チャレンジデータを用いる照合を行い、端末２１０から送られた生体情報信号２１１に対しては、全ユーザ照合を行うようにすればよい。

【００６０】

本実施例では、本発明の端末装置２００の使用割合が大きいほど平均のターンアラウンドタイムは短くなる。さらに、本発明の端末装置２００を使用する方が

レスポンスが短いため、本発明の端末装置２００の普及を促す効果もある。

【００６１】

（第４実施例）

端末装置からユーザ認証装置に対して生体情報そのものを送信する場合、盗聴などにより第三者に流出する可能性がある。生体情報はユーザに固有の生涯不変な情報であるため、パスワードなどのように、気軽に変更することができない。ネットワーク上での第三者への生体情報の流出を防ぐためには、生体情報を加工した情報を用いることが望ましい。加工した情報であれば、生体情報が流出した場合その情報を破棄し、別の方法で加工した情報に変更することができる。この加工は、加工データから元データに復元できない不可逆変換であることが望ましい。

【００６２】

例えば、指紋データにより本人認証を行う場合、指紋の文様の中にある端点、分岐点、断点などの特定のパターンそれぞれの相対位置などを用いて照合し、同一の指紋であるかどうか判定している。したがって、特定の位置の指紋画像を拡大する、あるいは縮小する、あるいは指紋画像の画素値を反転する、特定の位置の画像を入れ換える、別の指の指紋画像と一部を入れ換える、一部の領域を削除する、ダミーの指紋画像を挿入するなどの加工を行えば、加工した指紋データと元の指紋データとはパターンの種類も相対位置も全く異なるものができあがる。

【００６３】

図７に示すように、本実施例では、第１実施例に示したシステムにおいて、端末装置２００に、生体情報加工部２０５とその加工のための加工テーブルを格納する加工情報保持部２０６が備えられる。生体情報保持部２０１から出力される生体情報Ｂ１は、加工情報保持部２０６から出力された加工情報Ｍを基にして、生体情報加工部２０５により加工され、加工済み生体情報ＭＢ１として出力される。

ユーザ認証装置１００には、生体情報加工部１０４と加工情報保持部１０５が備えられ、辞書情報保持部から出力される生体情報辞書データＢを、加工情報保持部１０５に保持されている端末２００と同じ加工情報Ｍに基づいて、生体情報

加工部１０４により、加工済み生体情報辞書データＭＢに加工されて出力される。加工済み生体情報ＭＢ１と加工済み生体情報辞書データＭＢとは、ユーザ認証部で照合され、認証処理が行われる。

【００６４】

端末２００の加工情報保持部２０６及びユーザ認証装置１００の加工情報保持部１０５は、生体情報をどのように加工するかを示す同一の情報をテーブルとして保存しており、例えば、指紋画像に対して、次のようなＩＤが付された処理を行うことができる。

【００６５】

（ＩＤ）　（処理の内容）

０　：なにもしない。

１　：指紋画像の画素値の反転。

２　：指紋画像の拡大。

３　：指紋画像の縮小。

Ａ－Ｚ：同じ記号同士の画像の入れ替え。

ａ－ｚ：ａからｚのＩＤが割り振られたダミー指紋との置き替え。

指紋画像を５×５のブロックに分割して、ブロックごとに処理を行う場合、生体情報加工情報保持部２０６には、例えば以下に示すような２５個の加工情報が格納される。

【００６６】

１１０１Ａ２ＢａＢ１０３ｂＡ３０１Ｃ０３１２３Ｃｃ

これは、

第１ブロックを画素値反転し、

第２ブロックを画素値反転し、

第３ブロックは何もせず、

第４ブロックを画素値反転し、

第５ブロックを第１４ブロックと入れ換え、

第６ブロックを画像拡大し、

第７ブロックを第９ブロックと入れ換え、

第８ブロックにＩＤ＝ａのダミー指紋と入れ換え、

第１０ブロックを画素反転し、

：

第２５ブロックをＩＤ＝ｃのダミー指紋と入れ換える、

という処理を指紋画像データに対して行うことを表している。

この加工情報すなわち加工テーブルをユーザ認証装置１００と端末装置２００とで共有する。このように、ユーザ認証装置１００と端末装置２００とで、どのように加工したかの情報を共有しておけば、両者ともに同一の加工済み生体情報を生成することができる。ネットワーク上では、加工済みの生体情報を送信することで、たとえ加工済みの生体情報が漏洩したとしても、ユーザ本来の生体情報は漏洩せず、また、加工し直した生体情報を生成することで、従来通りユーザ認証を行うことができる。

【００６７】

本実施例では、加工テーブルは１種だけであるが、複数のテーブルを持っておき、生体情報の送信前に端末装置からユーザ認証装置に、あるいはユーザ認証装置から端末装置側にどのテーブルを使用するかの情報を送信し、それをもとに使用する加工テーブルを決定して生体情報の加工を行ってもよい。また、複数の加工テーブルを用いて、毎回異なる加工を行うことで、盗聴に対してよりセキュリティ強度の高いシステムを提供することができる。

【００６８】

もちろん、加工した生体情報であってもネットワーク上にそのまま送信するのではなく、ＶＰＮ（Virtual Private Network）やＳＳＬ（Secure Socket Layer）のようなネットワーク経路の暗号化や送信するデータそのものの暗号化により安全性を高めるとよい。

【００６９】

なお、本実施例では、ユーザ認証装置が要求した生体情報を送信するたびに加工を行うものとしたが、一度加工すればそれを記憶しておき、次回からは加工済みの生体情報を送信するようにすることもできる。

【００７０】

（第５実施例）

先の実施例では、生体情報保持部２０１には、各種の生体情報取得装置からの画像情報等をそのまま格納し、要求により必要な生体情報から特徴点を抽出して送信するか、又は生体情報そのものを送信し認証装置側で照合のために特徴点を抽出していた。本実施例では、生体情報取得部は、生体情報特徴点抽出装置３００として構成され、各種生体情報から予め特徴点を抽出し、特徴点の情報を端末装置２００の生体情報保持部２０１に保持するようにし、端末装置２００やユーザ認証装置１００における特徴点の抽出処理を省略する。

【００７１】

各種生体情報から予め特徴点を抽出する生体情報特徴点抽出装置３００は、例えば生体情報認証を必要とするサービスを行う店舗等に設置される。図８に示すように、生体情報特徴点抽出装置３００は、各種の生体情報センサ３０１－１、３０１－２、３０１－３及び各々の特徴点を抽出する特徴点抽出部３０２－１、３０２－２、３０２－３を有する。図には、説明のために３種類のセンサを示すが、センサ及び特徴点抽出部は３種類に限らない。生体情報センサ３０１－１、３０１－２、３０１－３では、それぞれ異なる生体情報を取得する。例えば生体情報センサ３０１－１では虹彩情報Ｂ１を取得し、生体情報センサ３０１－２では指紋情報Ｂ２を取得し、生体情報センサ３０１－３では静脈情報Ｂ３を取得する。各特徴点抽出部３０２－１、３０２－２、３０２－３は、得られた生体情報から各認証に即した特徴点Ｋ１，Ｋ２，Ｋ３を抽出する。

【００７２】

ユーザは、このような生体情報特徴点抽出装置３００に対して、本発明による端末２００を、無線あるいは有線で接続し、得られた特徴点データを端末装置２００の生体情報保持部２０１に入力し、格納する。そして、認証装置から生体情報Ｂ１の送信を要求された場合には、この特徴点データＫ１を送信する。なお、端末２００のセンサ２０２から出力される指紋情報Ｂ２１に対しても、生体情報保持部２０１からは指紋情報Ｂ２に対応する特徴点データＫ２が出力され、所有者認証部２０３での特徴点データへの変換を行わずに済む。ただし、センサ２０２からの指紋情報Ｂ２１に対しては、先の実施例と同様に特徴点データへの変換

が行われる。

【００７３】

本実施例では、特徴点データ生成を端末装置側で予め作成して保持しておき、要求された生体情報の特徴点データを端末装置からユーザ認証装置に送信することができる。したがって、認証処理にかかる時間を削減できる。すなわち、認証処理時間は、生体情報の取得にかかる時間と、特徴点抽出にかかる時間と、特徴点データと辞書データの照合にかかる時間との和であるが、本実施例では、予め特徴点データを抽出しておくことで、特徴点抽出時間を０にできる。

【００７４】

生体情報認証の精度は、生体情報の精度と特徴点データ抽出の精度に依存する。きれいな生体情報をセンサから取得し、ノイズ除去など前処理を行った後、特徴点を正確に抽出することで認証性能を向上させることができる。

【００７５】

きれいな生体情報の取得には精度の高いセンサが必要であるし、特徴点の正確な抽出には複雑な前処理などが必要になる。従来のシステムのように、各端末装置に高精度なセンサを備え、各端末装置あるいは認証装置で複雑な特徴点抽出処理を行うことは、システムの高コスト化や認証処理速度の低下を招く。本実施例では、取得場所に高精度なセンサを備えて、予め生体情報を取得しておく。したがって、高精度なセンサを各端末装置に備える必要がないため、システム全体のコストを削減できる。また取得時に取得装置により正確な特徴点抽出を行うから、端末装置側のＣＰＵの処理能力は低いものでよく、端末装置のコストを下げることができる。さらに、各認証処理において特徴点抽出処理を行わないため認証処理時間を短縮することができる。

【００７６】

なお、特徴点データも不可逆のデータであるため、元の生体情報を秘匿することができる。ただし、特徴点データであってもそのものを送信することは望ましくない。ダミーの特徴点を挿入する、一部の特徴点を削除するなどの加工を施すのが望ましい。

【００７７】

（第６実施例）

第２実施例では、端末装置からユーザ認証装置に送信される生体情報が常に同一であることを利用し、ユーザ認証装置においてチャレンジデータを生成して、生体情報が格納されている辞書データを特定するのに利用した。本実施例は、端末装置とユーザ認証装置ともに、同一のチャレンジデータを生成し、端末装置は、チャレンジデータをユーザ認証装置に送信し、ユーザ認証装置は、チャレンジデータ認証を行う。

【００７８】

図９に示すように、本実施例では、端末装置２２０には、第１実施例の端末装置に、生体情報保持部から出力される生体情報からチャレンジデータを生成するチャレンジデータ生成部２２４が追加され、生体情報送信部に代えてチャレンジデータ送信部２２５を備えている。

【００７９】

ユーザ認証装置１２０は、端末装置２２０に対してチャレンジデータを要求する要求信号を送信するチャレンジデータ要求部１２２と、正規ユーザのすべての生体情報である辞書データを格納する辞書情報保持部１２１と、辞書情報保持部１２１の生体情報データＢからチャレンジデータを生成するチャレンジデータ生成部１２３と、端末装置２２０から送信されたチャレンジデータとチャレンジデータ生成部１２３で生成されるチャレンジデータとを照合して本人認証を行うチャレンジデータ認証部１２４とを有する。

【００８０】

端末装置２００が、ユーザ認証装置からチャレンジデータの要求ＲＣを受信すると、端末装置２２０では、センサ２０２により入力されたユーザの指紋情報Ｂ２１と、生体情報保持部２１１に格納されている指紋情報Ｂ２とを照合して、所有者認証部２２３で本人認証を行う。操作者が所有者であると認証された場合、生体情報保持部から、ユーザ認証装置が必要としている虹彩情報Ｂ１を出力する。チャレンジデータ生成部２２２４は、出力された虹彩情報Ｂ１からチャレンジデータＣ１を生成し、このチャレンジデータＣ１をユーザ認証装置１２０に送信する。

【００８１】

ユーザ認証装置１２０では、辞書データの生体情報Ｂからチャレンジデータ Ｃを作成し、チャレンジデータ認証部１２４に送信する。チャレンジデータ認証部１２４では、受信したチャレンジデータＣ１と辞書データから生成されたチャレンジデータＣとを比較して一致するかどうかを検証する。一致すれば正規ユーザであるとして認証する。チャレンジデータによる認証は、生体情報認証のようにすべてのデータとの照合を行う必要はないので、認証結果が高速に得られる。

【００８２】

本実施例では、端末装置側、ユーザ認証装置側ともに生体情報を保持しておき、チャレンジデータが必要とされるときに生体情報からチャレンジデータを生成するようにしたが、予め生体情報からチャレンジデータを生成しておき、そのチャレンジデータを保持することもできる。

【００８３】

ただし、後述するように、端末装置からユーザ認証装置間で送受信されるチャレンジデータは、毎回異なる方が盗聴などに対してセキュリティ度が高い。毎回異なるチャレンジデータを生成するためには、その元となる生体情報を保持しておく必要がある。また、端末装置が複数のユーザ認証装置に対応する場合も、チャレンジデータはユーザ認証装置毎に異なる方が望ましい。したがって、予めチャレンジデータを生成しておくのではなく、ユーザ認証の都度、生体情報からチャレンジデータを生成することができるようにしておくのが望ましい。

【００８４】

（第７実施例）

前述したように、端末装置とユーザ認証装置間の送受信データは、毎回異なる方が盗聴などの不正アクセスに対する耐性が高い。そのために、本実施例では、チャレンジデータを生成する際に毎回異なるパラメータ（以下、「チャレンジパラメータ」という。）を用いてチャレンジデータを生成する。

本実施例では、チャレンジパラメータはユーザ認証装置から端末装置へ送られて、双方で同一のチャレンジデータを生成する。

【００８５】

図１０に示すように、本実施例では、第６実施例のユーザ認証装置１２０（図９）に、チャレンジパラメータ生成部１２５を付加し、チャレンジパラメータ生成部１２５が生成したチャレンジパラメータＣＰはチャレンジデータ生成部１２３に入力されるとともに、チャレンジデータ情報要求部１２２から端末装置２２０に送信され、チャレンジデータ情報送信部２２３を介して、端末装置２２０のチャレンジデータ生成部２２４に送られる。チャレンジパラメータＣＰに基づいて、端末２２０では、生体情報保持部２０１から選択された虹彩情報Ｂ１からチャレンジデータＣ２が生成され、ユーザ認証装置１２０に送信される。ユーザ認証装置１２０では、同一のチャレンジパラメータＣＰに基づいて、辞書情報保持部の虹彩情報Ｂからチャレンジデータ Ｃが生成される。このように、ユーザ認証装置１２０とユーザ端末２２０とは、共通のパラメータを用いて生体情報からチャレンジデータを生成する。チャレンジパラメータが異なれば、異なるチャレンジデータを作成できる。

【００８６】

チャレンジパラメータによるチャレンジデータの変換方法としては、例えば暗号化が考えられる。チャレンジパラメータ生成部１２５は例えばＤＥＳ（Data Encrypt Standard）の共通鍵を生成する機能を有しており、ここで生成した暗号鍵をチャレンジデータ生成部１２３に送信する。チャレンジデータ生成部１２３では、生体情報を該暗号鍵で暗号化し、その結果からＭＤ５などのチャレンジデータ生成アルゴリズムでチャレンジデータを生成する。ＤＥＳなどの暗号化アルゴリズムでは、暗号鍵が異なれば全く違う暗号データが生成される。暗号鍵を毎回変えることでチャレンジデータを毎回異なるものにすることができる。

【００８７】

暗号化処理が複雑である場合、単純に論理演算でもよい。４バイトのデータ列を生成しこのデータ列と生体情報とをＡＮＤやＯＲ、ＥｘＯＲなどの論理演算で変換してもよい。また、ＭＤ５のアルゴリズムを用いる場合であっても、１バイトのデータが相違すると、生成されるチャレンジデータは全く異なるものとなるから、使用されていない指紋画像データの一部を反転する、あるいは他の部分と入れ替えるというような、変換処理の指定をパラメータとすればよい。

【００８８】

これにより、通信経路上のデータを毎回異なるものにできるため、盗聴などの不正アクセスに対して安全性を高めることができる。

【００８９】

（第８実施例）

第７実施例ではユーザ認証装置１２０がチャレンジパラメータを生成していたが、本実施例では端末装置２２０がチャレンジパラメータを生成する。図１１に示すように、チャレンジパラメータ生成部２２６が、ユーザ端末装置２２０に設けられる。チャレンジパラメータ生成部２２６により生成されたチャレンジパラメータＣＰは、チャレンジデータ生成部２２４に送られるとともに、チャレンジデータ送信部を介してユーザ認証装置１２０に送られ、ユーザ認証装置１２０のチャレンジデータ生成部１２３によってチャレンジデータを生成する際のパラメータとして用いられる。このようにしても、端末２２０とユーザ認証装置１２０とで同一のチャレンジパラメータを用いて、毎回異なるチャレンジデータを生成することができ、本実施例も、第７実施例と同様、ネットワークにおける盗聴等に対する安全性を高めることができる。

【００９０】

なお、本発明によって生体情報から生成されるチャレンジデータは、本人固有のデータであるから、本人認証以外にも例えばシステム内に格納されている個人所有のファイル等の暗号化、復号化のための鍵として用いてもよい。

【００９１】

例えば、ユーザ認証後にユーザに提供されるサービスシステム（図示せず）において、ユーザがシステム内に個人情報やドキュメントなどを格納しておくことができるような場合、このチャレンジデータを鍵として個人情報やドキュメントなどを暗号化して格納しておくことが考えられる。このように個人情報を暗号化しておくと、個人情報の漏洩盗難などが防止でき、安全性を高めることができる。そして、ユーザ本人が暗号化されたファイルにアクセスしたい場合、ユーザ認証を行った後、ユーザの要求により、これらのファイルは、ユーザ認証に用いられたチャレンジデータを鍵として復号される。その結果、ユーザは自由にファイ

ルにアクセスできる。ユーザは暗号化・復号化の鍵を管理することなく、システム上の個人情報などを暗号化できるので、ユーザの管理負担が減少する。また、鍵となるチャレンジデータは端末装置の所有者認証がＯＫでなければ生成されないため、第三者には復号できないという利点がある。

【００９２】

第７および第８の実施例のようにチャレンジデータを毎回変える場合であっても、上記のようなファイル等の個人データの暗号化にチャレンジデータを使用することができる。すなわち、個人データを暗号化するチャレンジデータとして、次回の個人認証に用いられるチャレンジデータを用いるようにすればよい。換言すれば、個人データを暗号化するために作成されるチャレンジデータを次回の個人認証に用いるようにすればよい。このようにすれば、次回のユーザ認証をチャレンジデータを生成して行った後、ユーザ認証に用いたチャレンジデータを用いて、暗号化されているファイルを復号することができる。すなわち、ユーザが認証された際に、ユーザのデータは、今回ユーザ認証に用いたチャレンジデータで暗号化されているので、いったん、暗号化されているユーザのデータすべてを該チャレンジデータで復号する。さらに次回の認証の際に使用するチャレンジパラメータを設定し、これを元に次回のユーザ認証に用いられるチャレンジデータを生成し、ユーザのアクセス終了後、この次回のチャレンジデータを暗号鍵としてユーザのデータを暗号化すればよい。

【００９３】

（第９実施例）

現在、生体情報認証システムでは、同一の生体情報を使用する場合でも、どのようなフォーマットで使用するかなどの生体情報の規格は定められていない。そのため、指紋認証を例にすると、あるシステムでは３２０×３２０画素２５６階調（８ビット）モノクロの指紋画像による認証であり、また別のシステムでは２５６×３００画素二値（１ビット）画像による認証である。そのため本実施例では、ユーザ端末からユーザ認証装置に認証装置が要求するフォーマットに変換して生体情報を送信するようにした。このようにすれば、どのようなフォーマットの生体情報を用いるシステムにも対応することができる。

【００９４】

図１２に示すように、本実施例の構成は、本発明の第１実施例のユーザ認証装置１００に生体情報変換データ保持部１０６を追加し、端末装置２００に生体情報保持部から出力される生体情報を変換する生体情報変換部２０７を追加したものである。ただし、ユーザ認証装置における本人認証は、虹彩認証ではなく指紋認証であり、端末装置から送信される生体情報は、指紋情報である。

【００９５】

ユーザ認証装置１００の生体情報変換データ保持部１０６には、システムで使用している生体情報のフォーマットを変換データＴとして格納している。具体的には、画素数、階調数などの情報である。この変換データＴは、生体情報変換情報保持部１０６から生体情報要求部を介して、ユーザ端末２００に送信される。端末２００の生体情報変換部２０７では、送信された変換データＴを用いて生体情報保持部２０１からの生体情報Ｂ２を、認証装置が要求するフォーマットに変換し、変換生体情報ＴＢ２を生成する。

例えば、端末装置の生体情報保持部には３００×３００画素２５６階調の指紋画像が保持されていたとすると、ユーザ認証装置１００の生体情報変換情報保持部１０６に保持されている変換情報が解像度２５６×３２０画素２値であった場合、生体情報変換部２０７は、ユーザ認証装置から送られた変換データを基に、横方向の行の左右それぞれ１０ライン分追加して横方向のライン数を３２０画素に拡張し、縦方向の列の上下それぞれ２２ライン分削除して横方向のライン数を２５６画素に削減する。さらに２５６階調の指紋画像を２値画像に変換する。

このようにして、生体情報Ｂ２がユーザ認証装置１００が扱えるデータＴＢ２として変換され、ユーザ認証装置１００の要求に応じてユーザ認証装置１００に送信される。ユーザ認証装置１００の辞書情報保持部１０１では、指紋情報をユーザ認証装置１００が扱えるデータＴＢとして保持しているので、送信された指紋情報ＴＢ２と照合され、本人認証が行われる。このように、端末装置２００が保持している生体情報をユーザ認証装置１００が認証に使用できるフォーマットに変換できるため、どのようなフォーマットのユーザ認証にも対応することができる。

【００９６】

本実施例においては、毎回異なるチャレンジデータを生成するなどして盗聴などによる不正行為から情報を守る手だてを提供した。これらに加えて、さらに通信経路を暗号化することで、より盗聴などの不正行為による情報の流出を防ぐことができる。図示しないが、ユーザ認証装置側にＲＳＡの秘密鍵と公開鍵のペアを用意し、端末装置側に公開鍵を送信して端末装置からユーザ認証装置に送信する情報すべてを暗号化する。ユーザ認証装置では、暗号化された端末装置側からの情報を秘密鍵で復元する。公開鍵で暗号化したファイルは秘密鍵でしか復号できない。暗号化したこれら情報はユーザ認証装置のみが復元できるため、通信経路上の情報が盗聴されても情報が流出する危険性をなくすことができる。

【００９７】

（第１０実施例）

本発明によるユーザ端末には、ユーザ認証装置から生体情報を要求された場合に、ユーザ本人の要求された生体情報を格納していなければならず、また、ユーザ認証装置には、辞書データとして照合されるべき生体情報が保持されていなければならない。

【００９８】

端末装置内の生体情報保持部およびユーザ認証装置内の辞書データ保持部に格納する生体情報を収集するためには、ユーザがサービスを申し込む際に、サービス提供者の店舗などに赴いて、そこにある設備で生体情報を採取し、該サービスを利用する際のユーザ認証装置および端末装置に生体情報を格納するという方法が考えられる。しかしながら、サービス提供者毎に生体情報を取得する設備を設置しなければならないのは負担が大きい。また、現状では、同じ指紋認証を採用している複数のサービス提供者であっても、サービス提供者ごとに指紋情報を取得する設備を設置しなければならず、コスト増となっている。本実施例は、生体情報の取得及び利用をネットワークを介して行い、コストのかからない生体情報の取得及び利用のためのシステムを提供する。

【００９９】

図１３に示す本実施例の生体情報取得利用システムは、生体情報取得装置５０

０と端末装置１００とユーザ認証装置２００とを備える。生体情報取得装置５００は、指紋センサ、虹彩センサ、ＣＣＤカメラ等、各本人認証システムに用いられる各種生体情報を採取できるセンサ５０１－１～５０１－ｎと、暗号鍵５０２により暗号化を行う暗号化部を備えている。また、暗号化された情報を復号する復号鍵５０３を格納する復号鍵格納部を有する。１箇所の生体情報取得部で、使用されているすべての生体情報を取得できることが望ましい。生体情報取得部は、大規模な店舗内や駅前等に、証明写真撮影用のボックスと同様の形態に設けられることができる。

【０１００】

端末２００を所持したユーザが、生体情報取得装置５００において、備え付けの各種センサ５０１－１～５０１－ｎを用いて必要な生体情報データを入力する。入力された生体情報は、所定の暗号化鍵５０２で暗号化部により暗号化されて、ユーザの所持する端末２００の生体情報保持部２０１に格納される。

【０１０１】

また、格納に際して、端末２００は、生体情報取得装置５００にコネクタ等を介して接続されてもよいし、ブルートゥース等により無線で接続されてもよい。生体情報取得装置５００の使用料は、有料であっても無料であってもよい。ここでは、暗号化された生体情報を端末２００に格納するとしているので、以下に説明するように、得られた生体情報をネットワークで使用するときに、ユーザ認証装置１００又はユーザに課金することができる。暗号化しないで端末２００に格納する場合は、使用料を有料とすればよい。なお、生体情報取得装置５００の使用が終了すると、ユーザの生体情報データは、暗号化される前のものも暗号化された後のものも、生体情報取得装置５００から削除される。

【０１０２】

次に、ユーザが、インターネット上のサービス提供者にサービスの提供を申し込み、生体情報を本人認証に使用する場合には、ユーザは、端末２００に格納した暗号化済みの生体情報をサービス提供者のユーザ認証装置１００に送信する。サービス提供者は前記生体情報取得装置５００ないしその管理者に対して、暗号化データを復号する復号鍵５０３の提供を要求する。生体情報取得装置５００は

対価と引き換えにユーザ認証装置に復号鍵５０３を提供する。

【０１０３】

端末２００を所持しているユーザから対価を要求する場合も考えられる。この場合は、端末２００からの要求で対価と引き換えに復号鍵５０３が端末に提供される。端末で復号された生体情報データは、そのままユーザ認証装置１００に送信され使用される。

【０１０４】

これにより、生体情報の採取のサービスを提供する生体情報取得システムは、採取したユーザの生体情報がユーザの認証として用いられる際にサービス提供者又は端末所有者より対価を得ることができる。また、図示しないが、認証ごとに対価を得るようにしてもよい。すなわち生体情報の使用回数に応じて対価を支払うシステムであってもよい。

【０１０５】

これら生体情報取得システムにより、サービス提供者は生体情報を取得するための設備を所有する必要がなく、低コストで生体情報認証システムを構築することができる。また、生体情報取得システムはサービス提供者から対価を得ることで生体情報取得によるビジネスを成立させることができる。

【０１０６】

生体情報取得システムが採取した生体情報は、さまざまな生体情報認証で用いられる可能性がある。したがって、高精度な認証ができるよう、ノイズ除去などの前処理や特徴点を抽出しやすくする境界強調などを施した、生体情報認証しやすいデータをユーザ、ユーザ認証装置に提供するようにする。

【０１０７】

このようにすれば、サービス提供者は、物理的な店舗を有することなく、ネットワークを利用してユーザにサービスを提供することができ、物理的な距離に関係なくどの場所にいるユーザに対してもサービスを提供できる。

【０１０８】

以上述べた本発明の実施の態様は、以下のとおりである。

【０１０９】

（付記１）本人に係る複数の生体情報を格納した生体情報保持部を備え、少なくとも一つの前記生体情報が、当該本人の認証に使用される端末装置。

（付記２）前記生体情報は、複数種類の生体情報を含む付記１に記載の端末装置。

（付記３）前記生体情報は、生体情報から抽出された特徴点情報である付記１に記載の端末装置。

（付記４）前記生体情報は、暗号化された生体情報である付記１に記載の端末装置。

（付記５）本人認証が行われるとき、前記生体情報保持部から前記本人認証に使用される生体情報を選択して出力する付記１～４のいずれか一項に記載の端末装置。

（付記６）本人に係る複数の生体情報を格納した生体情報保持部と、

生体情報を取得する生体情報取得部と、

前記取得した生体情報と前記生体情報保持部に格納された生体情報に基づき前記本人認証を行う本人認証部と、

前記本人認証部で本人と認証された場合に、前記生体情報保持部から所定の生体情報を選択して出力する生体情報出力部と

を備える端末装置。

（付記７）前記生体情報保持部から選択された前記生体情報を少なくとも部分的に編集加工する生体情報加工部を備え、該編集加工された生体情報を出力する付記６に記載の端末装置。

（付記８）前記生体情報保持部から選択された生体情報のフォーマットを変換する生体情報変換部を備え、該フォーマット変換された生体情報を出力する付記６又は７に記載の端末装置。

（付記９）前記生体情報保持部から選択された前記生体情報を、該生体情報に対応する特定のビット長からなる生体情報対応データを生成する生体情報対応データ生成部を備え、

該生成された生体情報対応データを前記生体情報送信部より送信する付記６～８のいずれか１項に記載の端末装置。

（付記１０）前記生体情報対応データを生成するために使用されるパラメータを生成する生体情報対応データパラメータ生成部を備える付記９に記載の端末装置。

（付記１１）本人に係る複数の生体情報を格納する生体情報保持部と、少なくとも一つの前記生体情報を送信する生体情報送信部とを有する端末装置と、

生体情報を照合すべき辞書情報として保持する辞書情報保持部と、前記生体情報送信部から送信される前記生体情報と前記辞書情報保持部に格納されている辞書情報とに基づいて第１の本人認証を行う第１本人認証部を有する認証装置と

を備えた生体情報認証システム。

（付記１２）前記生体情報は、複数種類の生体情報を含む付記１１に記載の生体情報認証システム。

（付記１３）前記端末装置は、生体情報を取得する生体情報取得部と、第２の本人認証を行う第２本人認証部とを備え、

前記取得された生体情報と前記生体情報保持部に格納された生体情報とを用いて第２の本人認証を行い、当該本人と認証された場合に、前記第１本人認証部において使用する生体情報を前記生体情報送信部より前記認証装置に送信する付記１１又は１２に記載の生体情報認証システム。

（付記１４）前記認証装置は、前記端末装置から送信される前記生体情報に基づいて前記生体情報に対応する特定のビット長からなる生体情報対応データを生成する生体情報対応データ生成部を備え、

該生成された生体情報対応データにより前記辞書情報保持部に格納されている辞書情報を特定し、前記第１本人認証部において、該特定された辞書情報と前記送信された生体情報とに基づいて本人認証を行う付記１１～１３のいずれか一項に記載の生体情報認証システム。

（付記１５）前記認証装置は、前記特定された辞書情報に基づく本人認証が実行できない場合、前記辞書情報保持部に格納されたすべての辞書情報と前記送信された生体情報とに基づいて本人認証を行う付記１４に記載の生体情報認証システム。

（付記１６）前記端末装置は、前記生体情報保持部から選択された前記生体情

報を少なくとも部分的に編集加工する第１生体情報加工部と、前記第１生体情報加工部による編集加工のための情報を格納する第１生体情報加工情報保持部とを有し、

前記認証装置は、前記辞書情報を少なくとも部分的に編集加工する第２生体情報加工部と、前記第２生体情報加工部による編集加工のための情報を格納する第２生体情報加工情報保持部とを有し、

編集加工された前記生体情報と編集加工された前記辞書情報とに基づいて、第１本人認証部で本人認証を行う付記１１～１５に記載の生体情報認証システム。

（付記１７）前記認証装置は、第１本人認証部で使用する生体情報のフォーマット情報を格納する変換情報保持部を備え、

前記端末装置は、前記生体情報保持部に格納された前記生体情報のフォーマットを変換する生体情報変換部を備え、

前記生体情報変換部は、前記変換情報保持部から送信された前記フォーマット情報を用いて前記生体情報のフォーマットを変換し、該フォーマット変換された前記生体情報を前記認証装置に送信する付記１１～１６のいずれか一項に記載の生体情報認証システム。

（付記１８）本人に係る複数の生体情報を格納する生体情報保持部と、前記生体情報保持部に格納された複数の生体情報から選択された前記生体情報に対応する特定のビット長からなる生体情報対応データを生成する第１生体情報対応データ生成部と、該生成された第１生体情報対応データを送信する生体情報対応データ送信部とを有する端末装置と、

生体情報を照合すべき辞書情報として保持する辞書情報保持部と、前記辞書情報に対応する特定のビット長からなる生体情報対応データを生成する第２生体情報対応データ生成部と、送信された前記第１生体情報対応データ及び第２生体情報対応データに基づいて第１の本人認証を行う第１本人認証部を有する認証装置と

を備えた生体情報認証システム。

（付記１９）前記端末装置は、生体情報を取得する生体情報取得部と、第２の本人認証を行う第２本人認証部とを備え、

前記取得された生体情報と前記生体情報保持部に格納された生体情報とを用いて第２の本人認証を行い、本人と認証された場合に前記認証装置の第１本人認証部において使用する第１生体情報対応データを前記認証装置に送信する付記１８に記載の生体情報認証システム。

（付記２０）前記端末装置は、前記生体情報対応データを生成するために使用される生体情報対応データパラメータを生成する第１生体情報対応データパラメータ生成部を備え、

前記生成された生体情報対応データパラメータは、前記第１生体情報対応データ生成部において使用されるとともに、前記認証装置に送信され、前記第２生体情報データ生成部においても使用される付記１８又は１９に記載の生体情報認証システム。

（付記２１）前記認証装置は、前記生体情報対応データを生成するために使用される生体情報対応データパラメータを生成する第２生体情報対応データパラメータ生成部を備え、該生成された生体情報対応データパラメータは、前記第２生体情報対応データ生成部において使用されるとともに、前記端末装置に送信され、前記第１生体情報データ生成部においても使用される付記１８又は１９に記載の生体情報認証システム。

（付記２２）前記認証装置は、本人が所有する情報を当該本人の認証に用いた前記生体情報対応データを鍵として暗号化する付記１８に記載の生体情報認証システム。

（付記２３）本人に係る複数種類の生体情報を取得するための生体情報取得部と、前記生体情報取得部により取得した生体情報を端末装置に格納する生体情報格納部とを備える生体情報取得装置。

（付記２４）前記生体情報格納部は、前記取得した生体情報から生体情報の特徴点を抽出して前記端末装置に格納する付記２３に記載の生体情報取得装置。

（付記２５）前記生体情報格納部は、前記取得した生体情報を暗号化して前記端末装置に格納する付記２３に記載の生体情報取得装置。

【０１１０】

（付記２６）本人に係る複数の生体情報を格納する生体情報保持部を有する端

末装置と、

前記端末装置から送信される前記生体情報に基づいて本人認証を行う認証装置と、

前記生体情報を取得するための生体情報取得部と該生体情報を暗号鍵により暗号化する暗号化部と復号鍵を格納する復号鍵格納部とを有する生体情報取得装置とを備え、

前記生体情報取得部により取得された前記本人に係る生体情報は、前記暗号化部で暗号化して前記端末装置の前記生体情報保持部に格納され、前記端末装置に格納された前記暗号化された生体情報が前記認証装置に送信されたときに、該認証装置において前記生体情報取得装置の前記復号鍵格納部に格納された前記復号鍵を使用して前記暗号化された生体情報を復号する生体情報取得システム。

（付記２７）前記生体情報取得装置は、前記認証装置において前記復号鍵が使用されたとき、当該使用に対して前記認証装置に課金する付記２３に記載の生体情報取得システム。

（付記２８）前記生体情報取得装置は、該生体情報取得装置によって端末装置に格納された前記生体情報が前記認証装置で使用された使用回数に応じて、前記認証装置に課金する付記２３に記載の生体情報取得システム。

【図面の簡単な説明】

【図１】

本発明による認証端末装置の基本形を示す図である。

【図２】

本発明の第１実施例を示す図である。

【図３】

本発明の第１実施例の動作フロー（その１）を示す図である。

【図４】

本発明の第１実施例の動作フロー（その２）を示す図である。

【図５】

本発明の第２実施例を示す図である。

【図６】

本発明の第３実施例を示す図である。

【図７】

本発明の第４実施例を示す図である。

【図８】

本発明の第５実施例を示す図である。

【図９】

本発明の第６実施例を示す図である。

【図１０】

本発明の第７実施例を示す図である。

【図１１】

本発明の第８実施例を示す図である。

【図１２】

本発明の第９実施例を示す図である。

【図１３】

本発明の第１０実施例を示す図である。

【図１４】

従来の生体情報認証システムの１例を示す図である。

【図１５】

従来の生体情報認証フローを示す図である。

【符号の説明】

１０，２００，２２０…認証端末装置

１，２０１…生体情報保持部

２，２０２…生体情報センサ

３，２０３…所有者認証部

４，２０４…生体情報送信部

１００，１２０…認証端末装置

１０１…辞書情報保持部

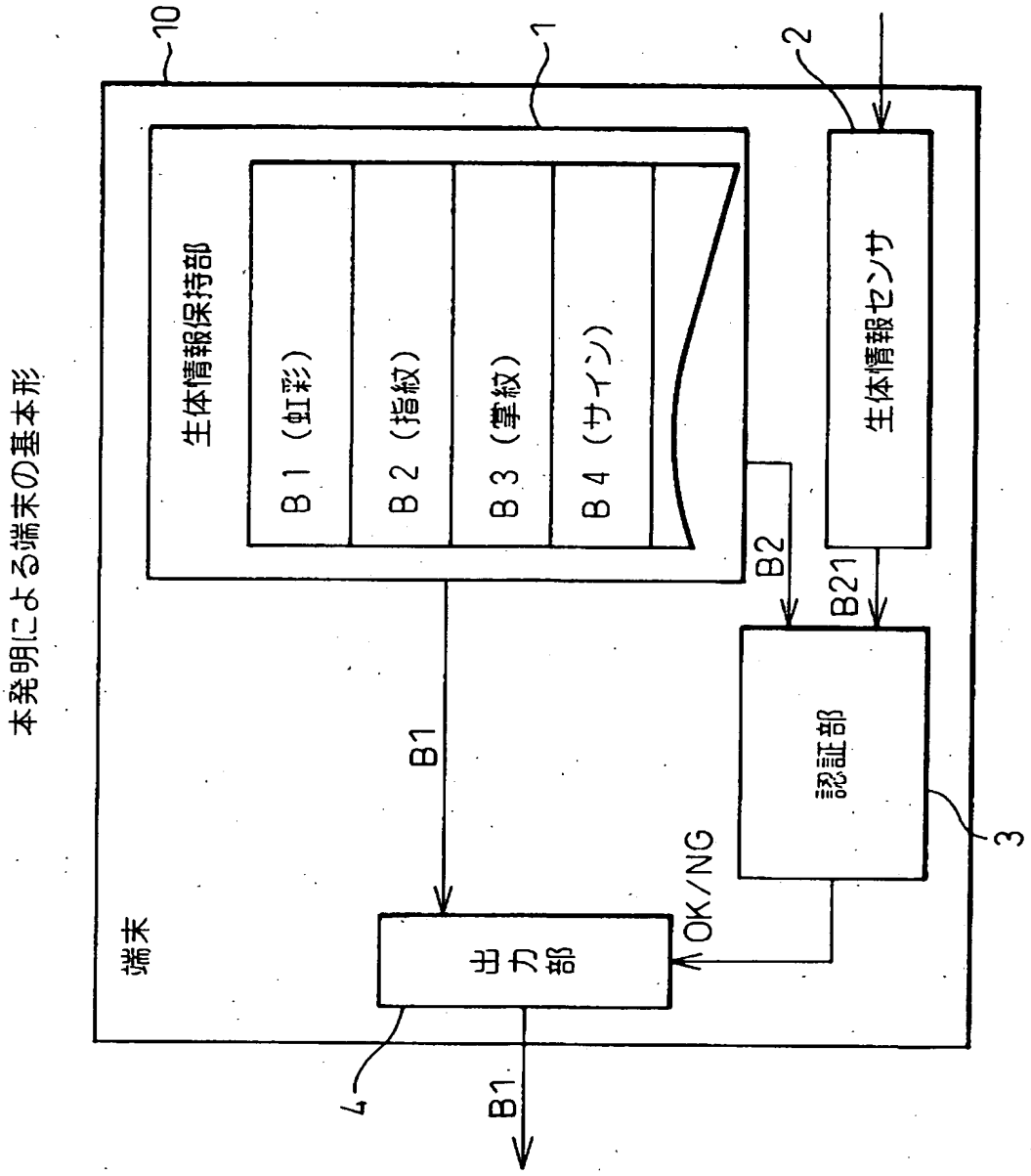
１０２…生体情報要求部

１０３…ユーザ認証部

【書類名】　図面

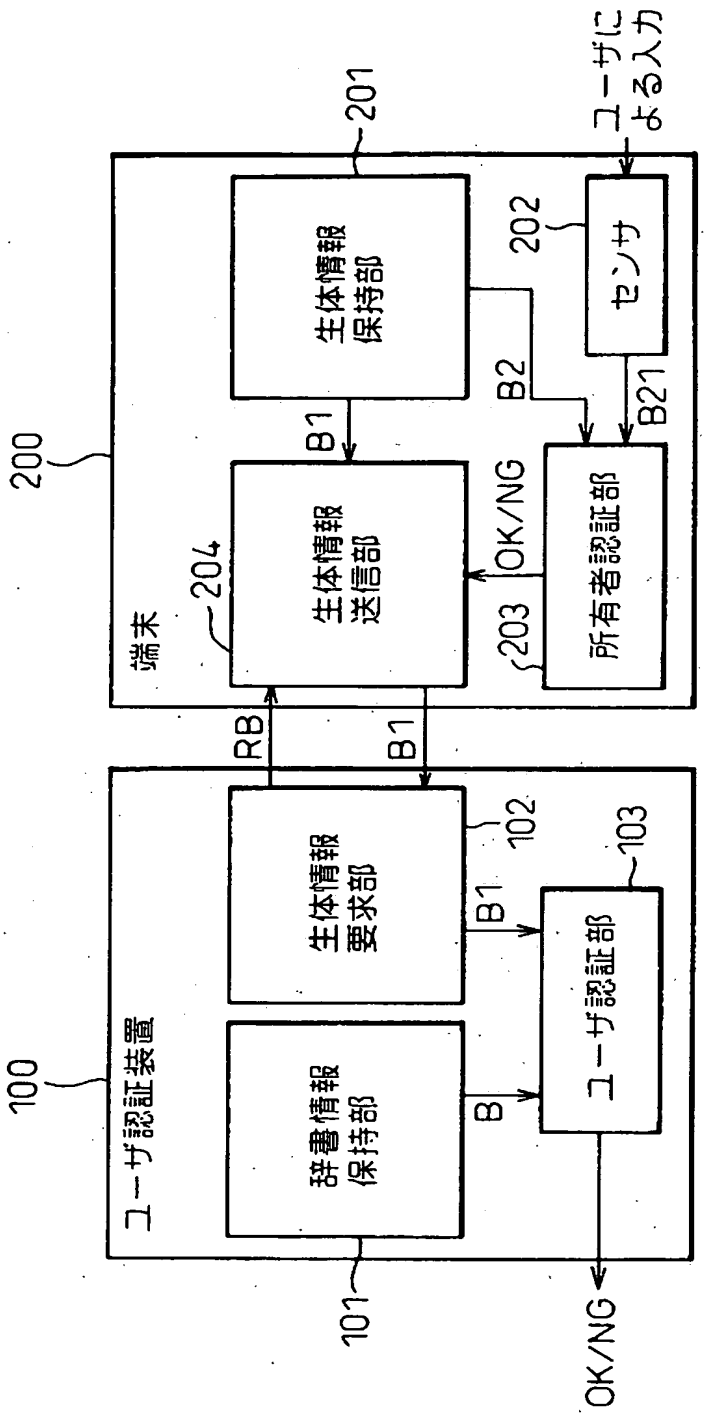
【図１】

図１


本発明による端末の基本形
10
1
2
生体情報保持部
B１（虹彩）
B２（指紋）
B３（掌紋）
B４（サイン）
生体情報センサ
B2
B21
B1
認証部
3
OK/NG
出力部
4
B1
端末

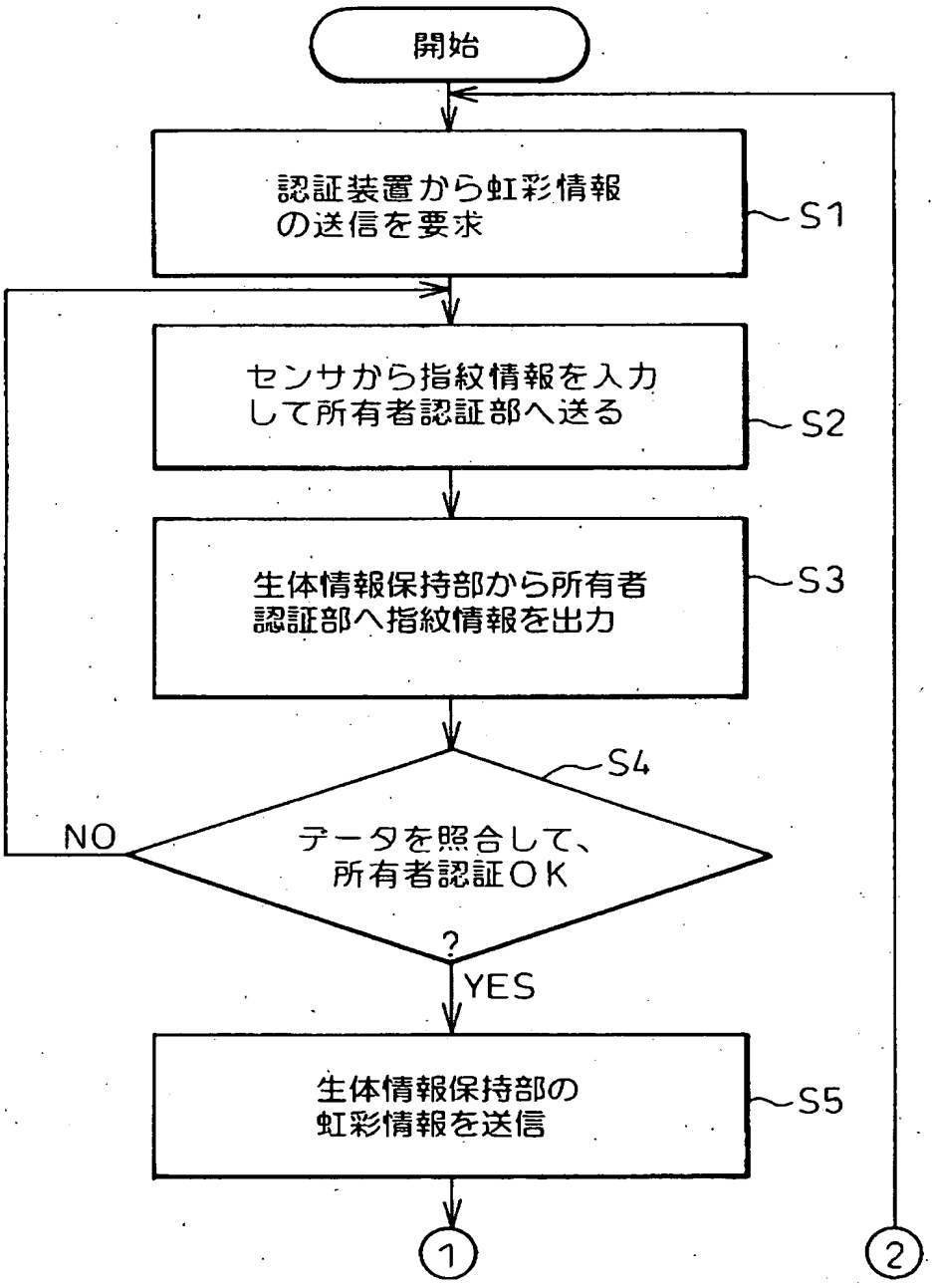
【図２】

図２


第１実施例
ユーザ認証装置
100
端末
200
生体情報保持部
201
センサ
202
所有者認証部
203
生体情報送信部
204
生体情報要求部
102
ユーザ認証部
103
辞書情報保持部
101
ユーザによる入力
B1
B2
B21
OK/NG
RB
B
OK/NG

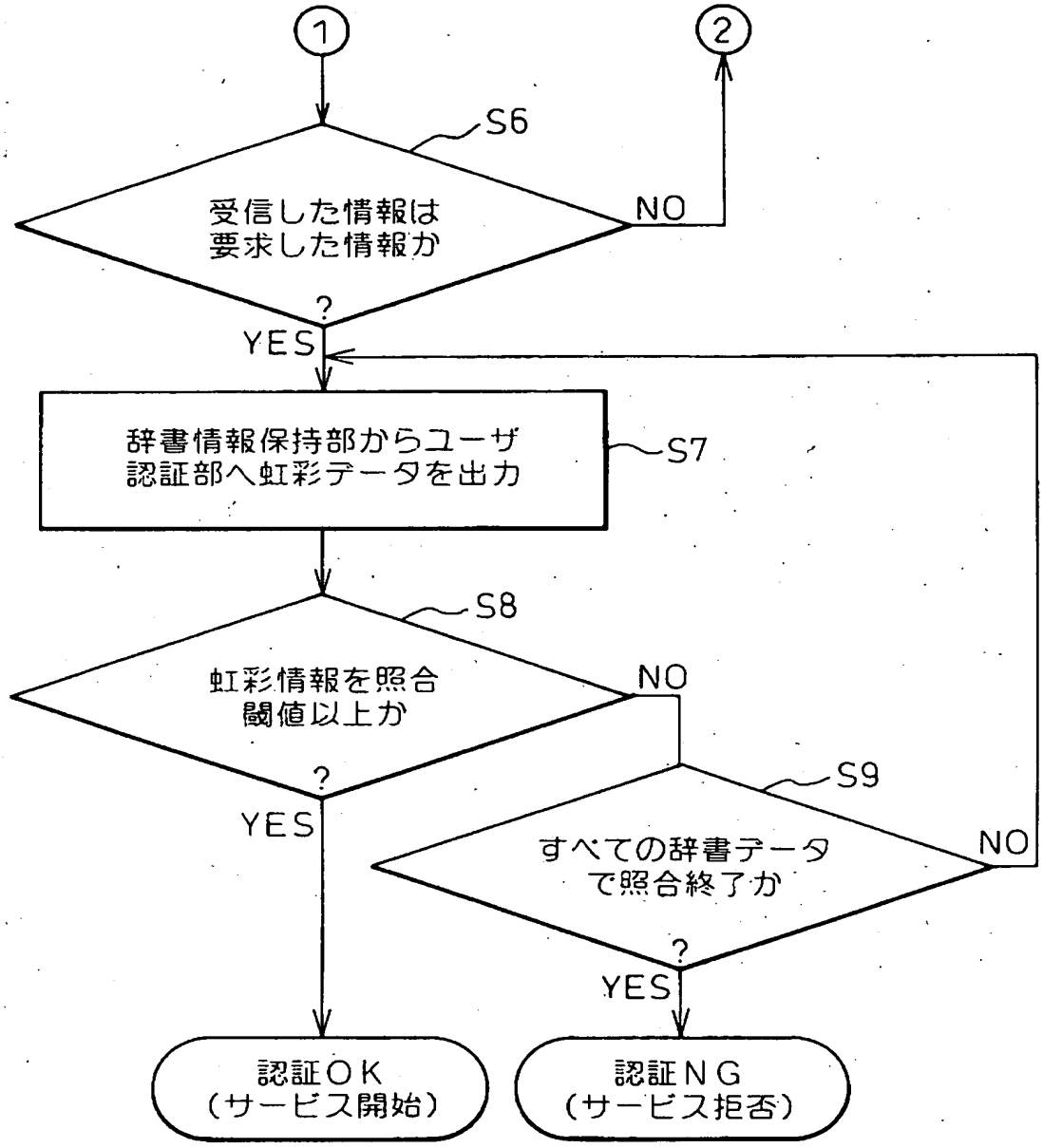
【図３】

図 3　　第１実施例のフロー（その１）



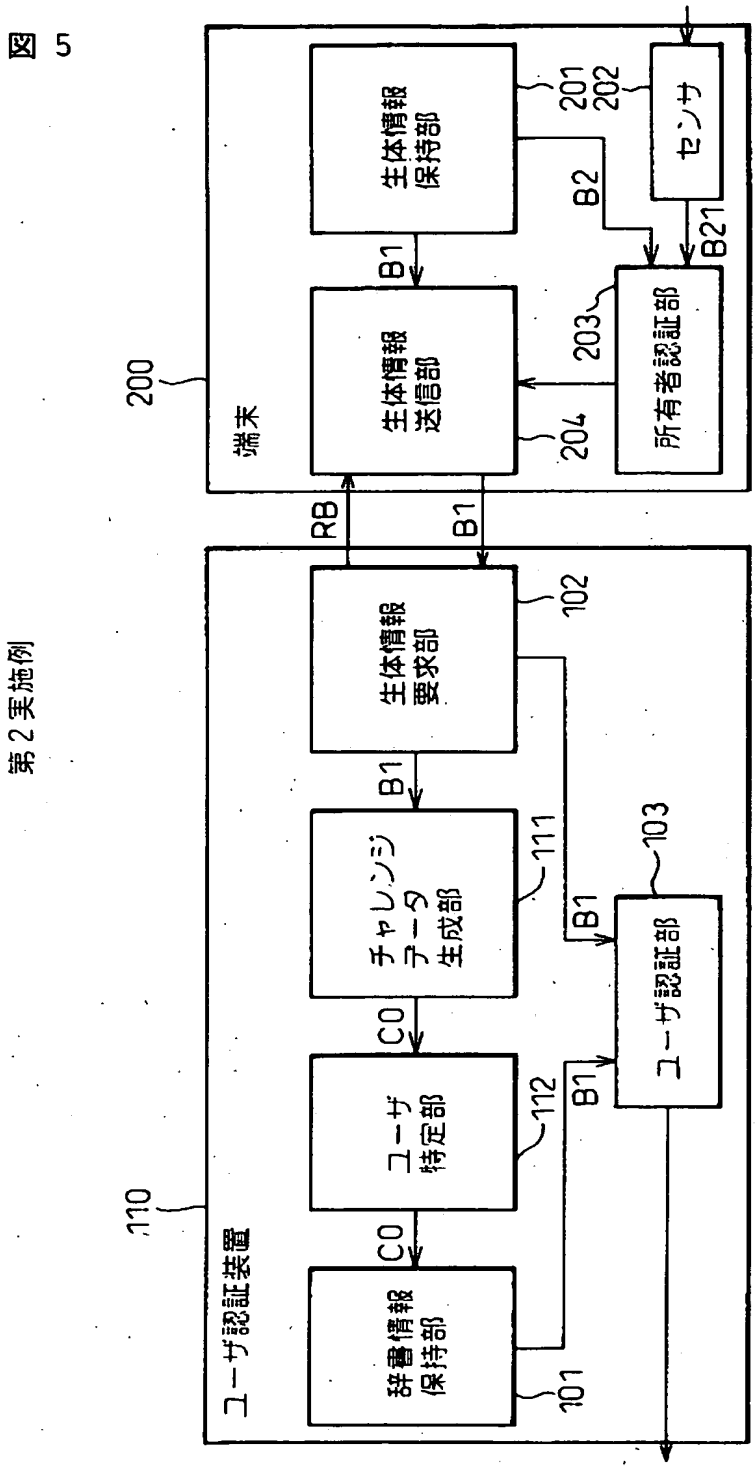
【図４】

図 4　　第１実施例のフロー（その２）



【図５】

図 5


第２実施例
ユーザ認証装置
110
辞書情報保持部
101
ユーザ特定部
112
チャレンジデータ生成部
111
生体情報要求部
102
ユーザ認証部
103
C0
C0
B1
B1
B1
RB
端末
200
生体情報送信部
204
生体情報保持部
201
センサ
202
所有者認証部
203
B1
B2
B21

【図６】

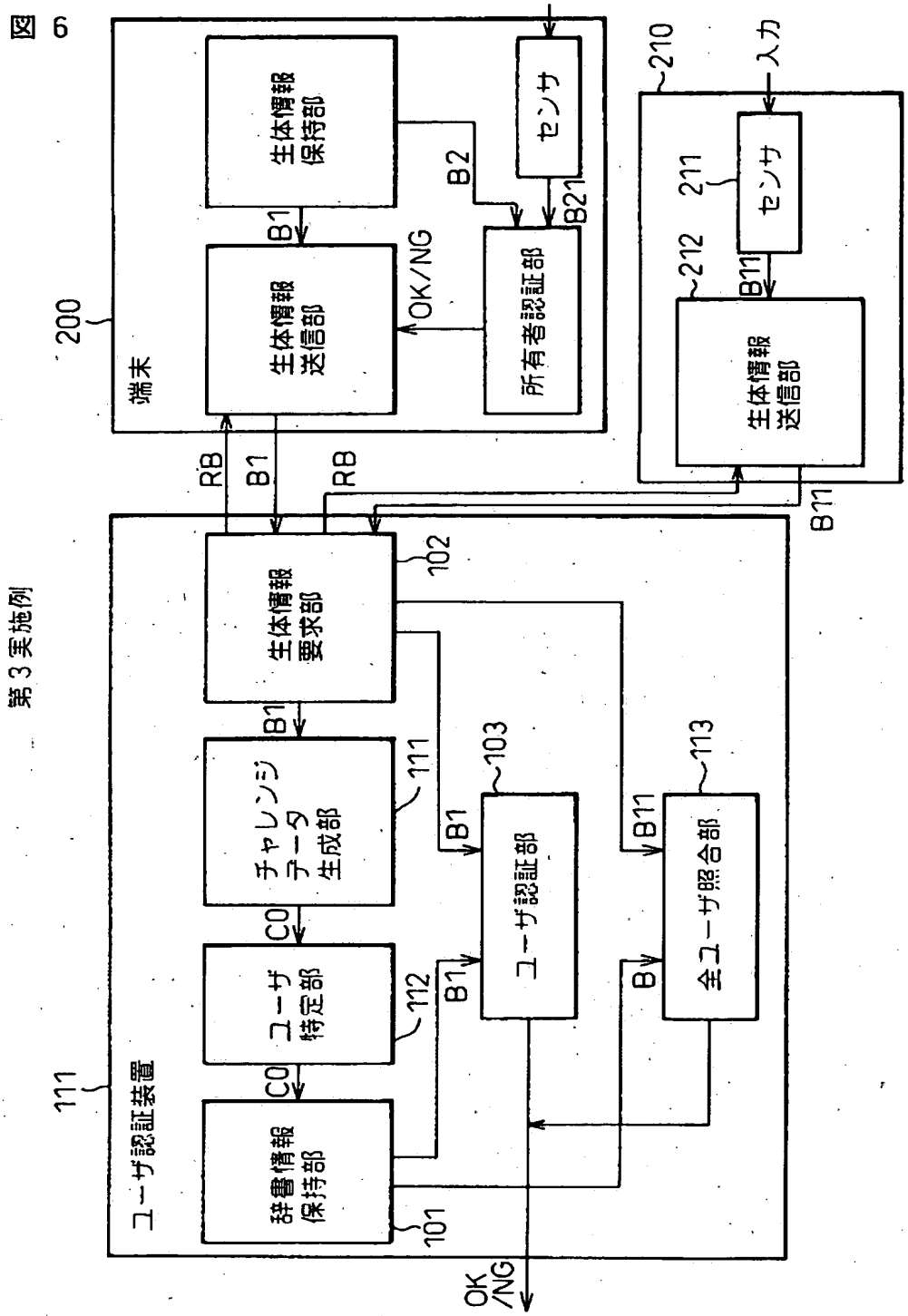


図 6
第３実施例
端末
200
生体情報保持部
センサ
B2
B21
B1
生体情報送信部
OK/NG
所有者認証部
210
入力
211
センサ
212
B11
生体情報送信部
RB
B1
RB
B11
ユーザ認証装置
111
生体情報要求部
102
B1
チャレンジデータ生成部
111
C0
ユーザ特定部
112
C0
辞書情報保持部
101
B1
ユーザ認証部
103
B
全ユーザ照合部
113
B11
OK/NG

【図７】

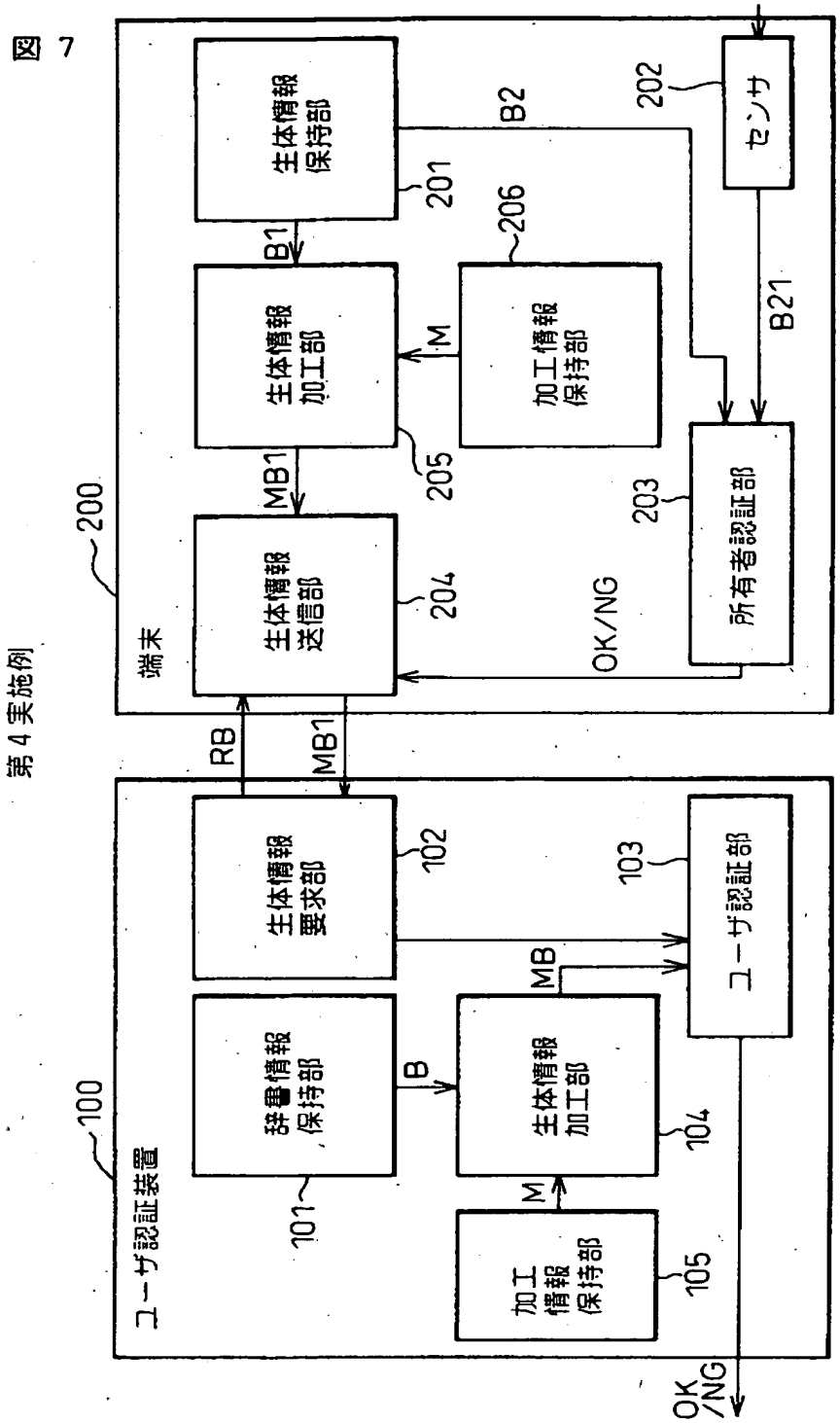
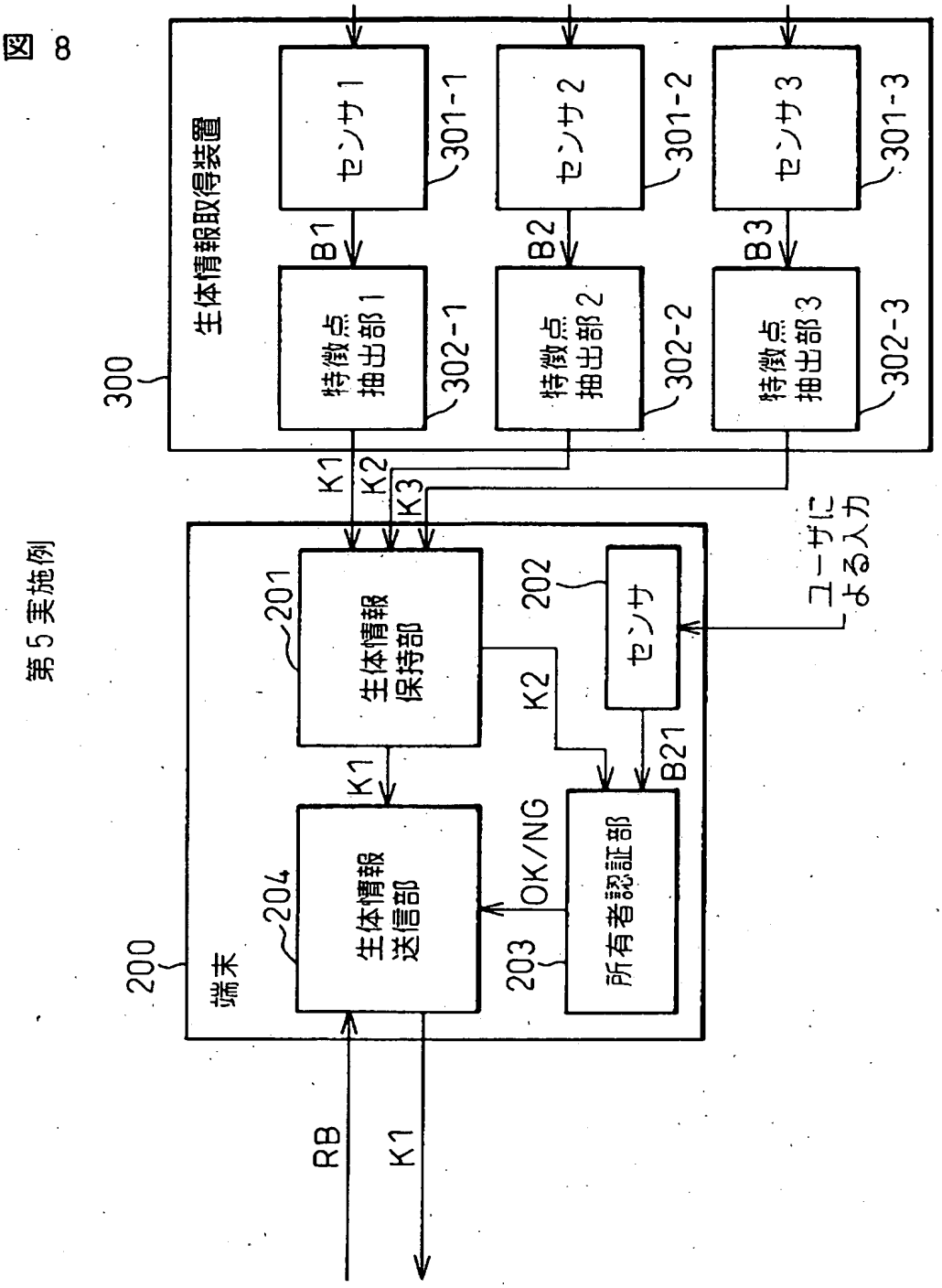


図 7
第４実施例
端末
200
生体情報保持部
201
B2
202
センサ
B1
206
生体情報加工部
M
加工情報保持部
B21
MB1
205
203
所有者認証部
生体情報送信部
204
OK/NG
RB
MB1
ユーザ認証装置
100
生体情報要求部
102
103
ユーザ認証部
MB
辞書情報保持部
B
生体情報加工部
104
101
M
加工情報保持部
105
OK/NG

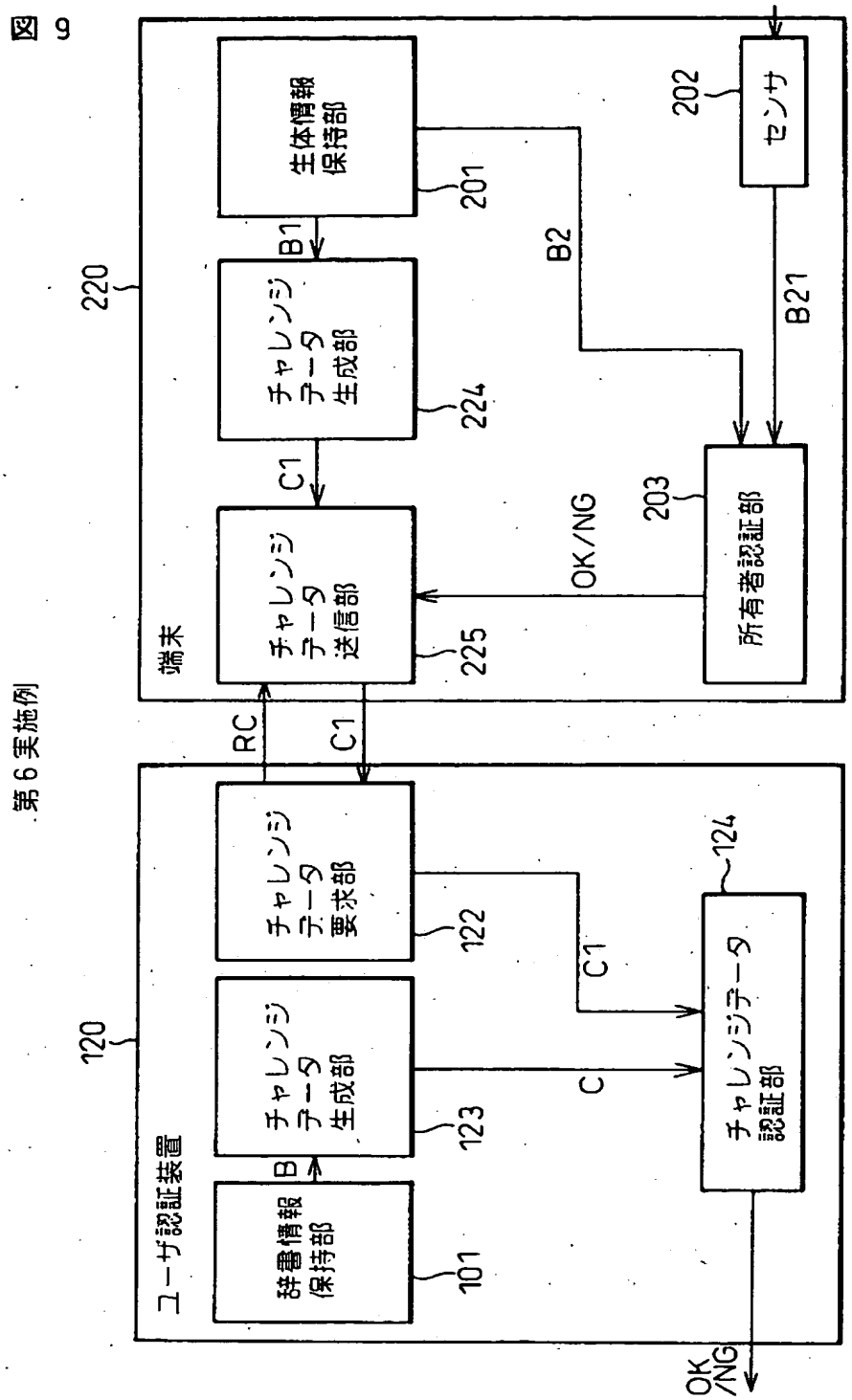
【図８】

図 8


第５実施例
生体情報取得装置
300
センサ１
センサ２
センサ３
301-1
301-2
301-3
B1
B2
B3
特徴点抽出部１
特徴点抽出部２
特徴点抽出部３
302-1
302-2
302-3
K1
K2
K3
ユーザによる入力
端末
200
生体情報保持部
201
センサ
202
生体情報送信部
204
所有者認証部
203
K1
K2
B21
OK/NG
RB
K1

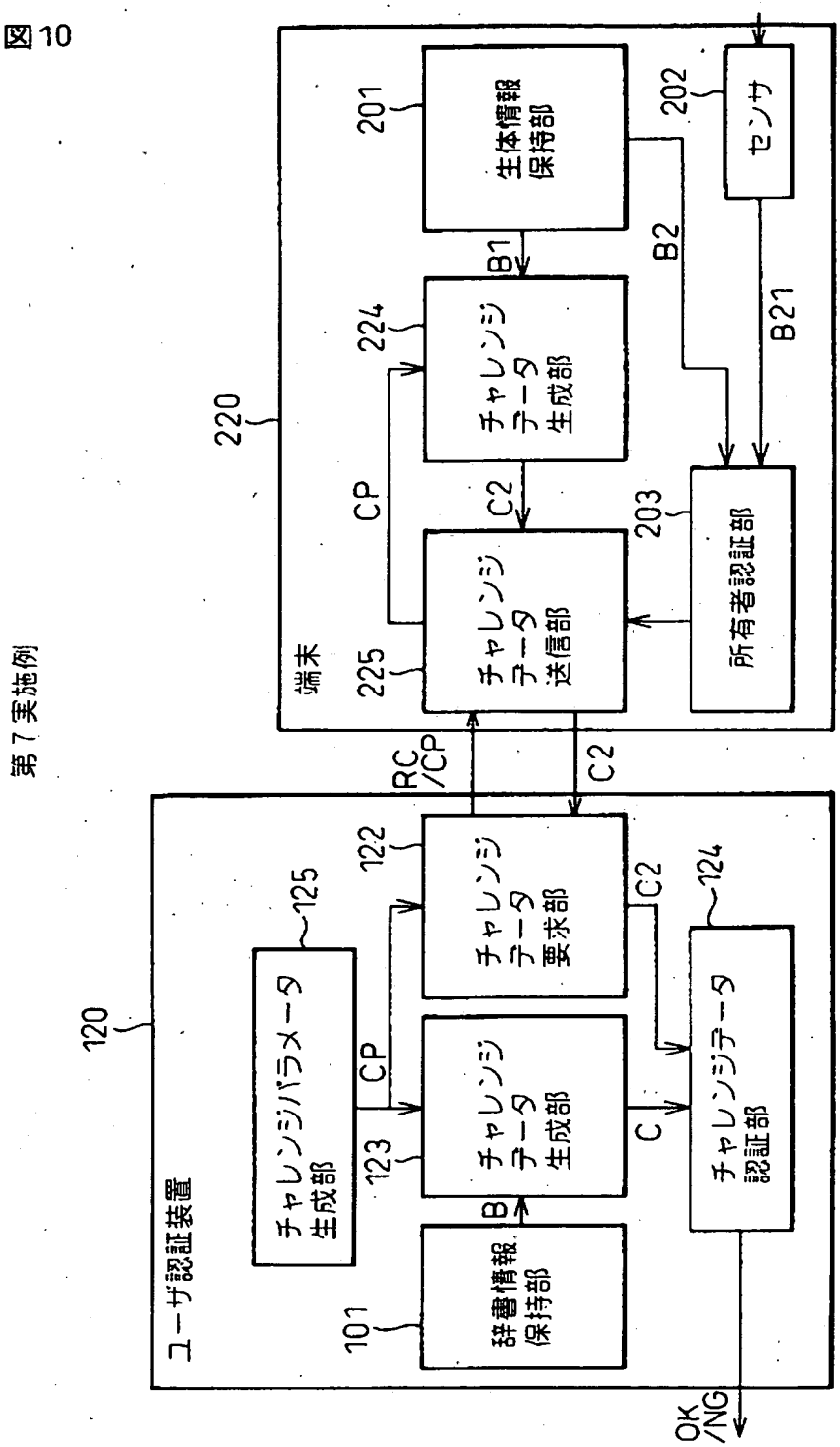
【図９】

図 9


第６実施例
端末
220
生体情報保持部
201
B1
チャレンジデータ生成部
224
C1
チャレンジデータ送信部
225
B2
センサ
202
B21
所有者認証部
203
OK/NG
RC
C1
ユーザ認証装置
120
チャレンジデータ要求部
122
C1
チャレンジデータ生成部
123
C
B
辞書情報保持部
101
チャレンジデータ認証部
124
OK/NG

【図１０】

図10


第７実施例
ユーザ認証装置
120
辞書情報保持部
101
チャレンジパラメータ生成部
125
チャレンジデータ生成部
123
チャレンジデータ要求部
122
チャレンジデータ認証部
124
B
CP
C
C2
RC/CP
C2
OK/NG
端末
220
生体情報保持部
201
センサ
202
所有者認証部
203
チャレンジデータ送信部
225
チャレンジデータ生成部
224
B1
B2
B21
CP
C2

【図１１】

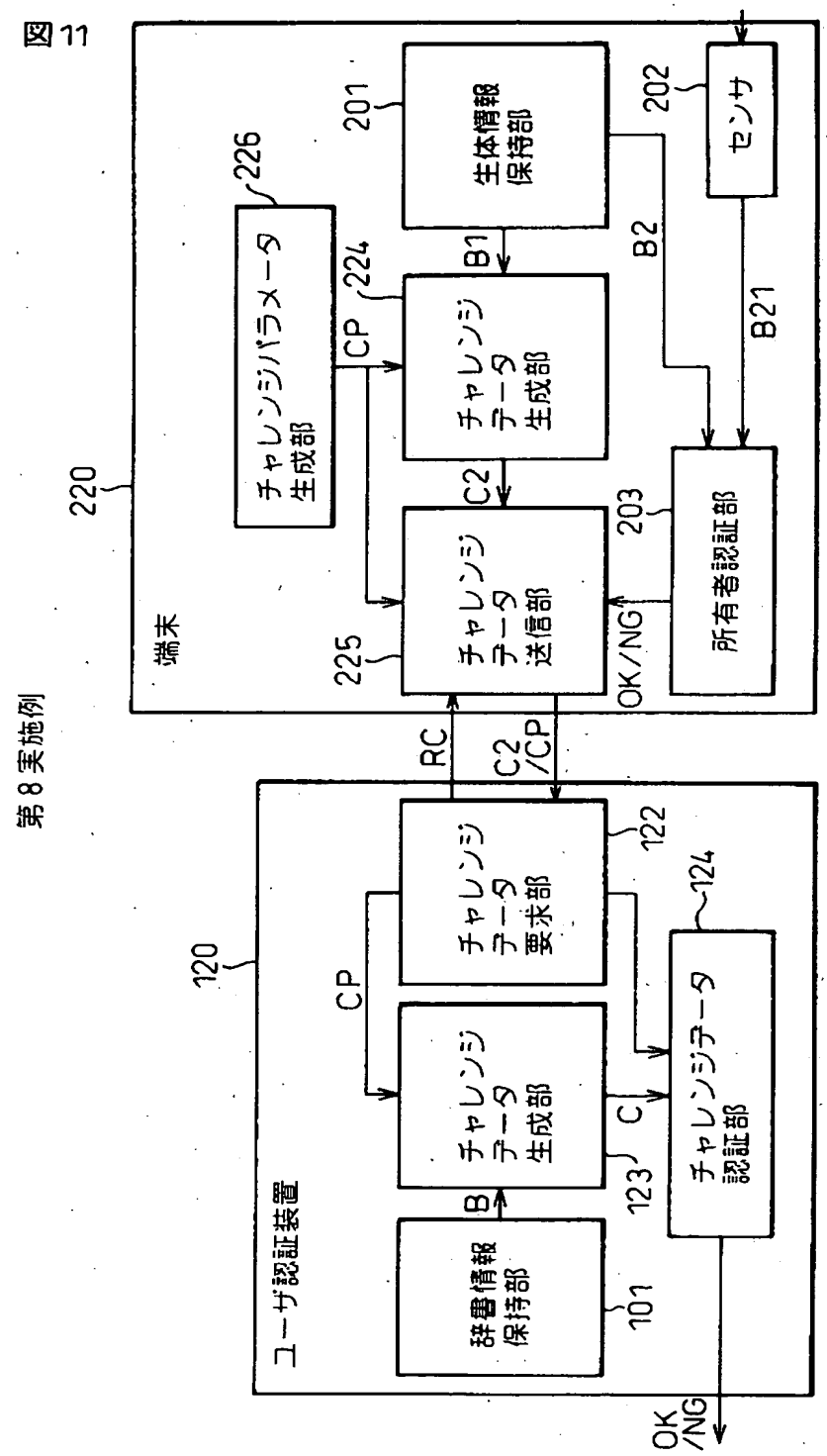
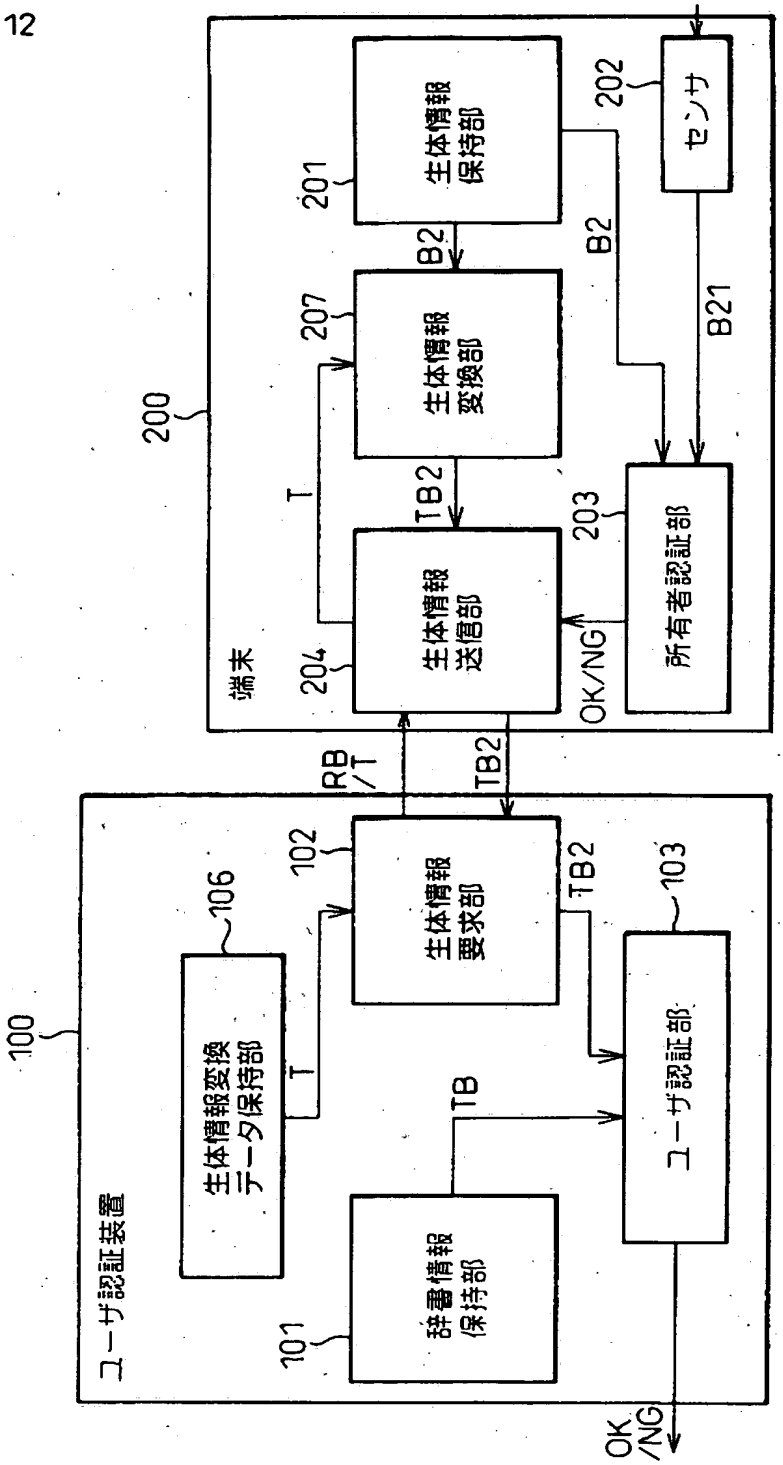


図11
第8実施例
端末
220
生体情報保持部
201
センサ
202
チャレンジパラメータ生成部
226
チャレンジデータ生成部
224
CP
B1
B2
B21
C2
チャレンジデータ送信部
225
所有者認証部
203
OK/NG
RC
C2/CP
ユーザ認証装置
120
チャレンジデータ要求部
122
124
CP
チャレンジデータ生成部
C
123
チャレンジデータ認証部
B
辞書情報保持部
101
OK/NG

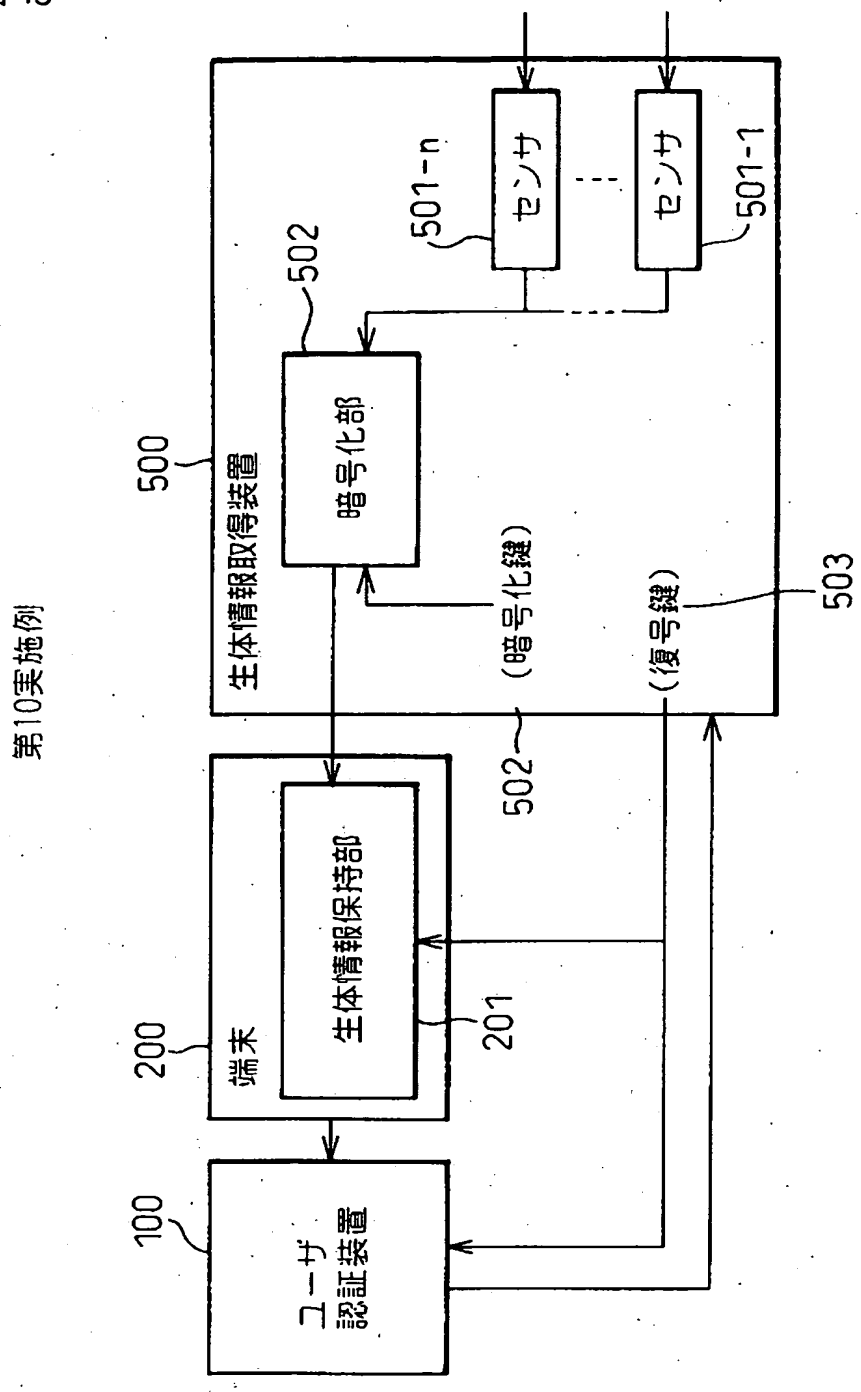
【図１２】

図 12


第９実施例
ユーザ認証装置
100
端末
200
生体情報保持部
201
センサ
202
生体情報変換部
207
所有者認証部
203
生体情報送信部
204
生体情報要求部
102
ユーザ認証部
103
生体情報変換データ保持部
106
辞書情報保持部
101
B2
B21
TB2
T
TB
RB/T
OK/NG

【図１３】

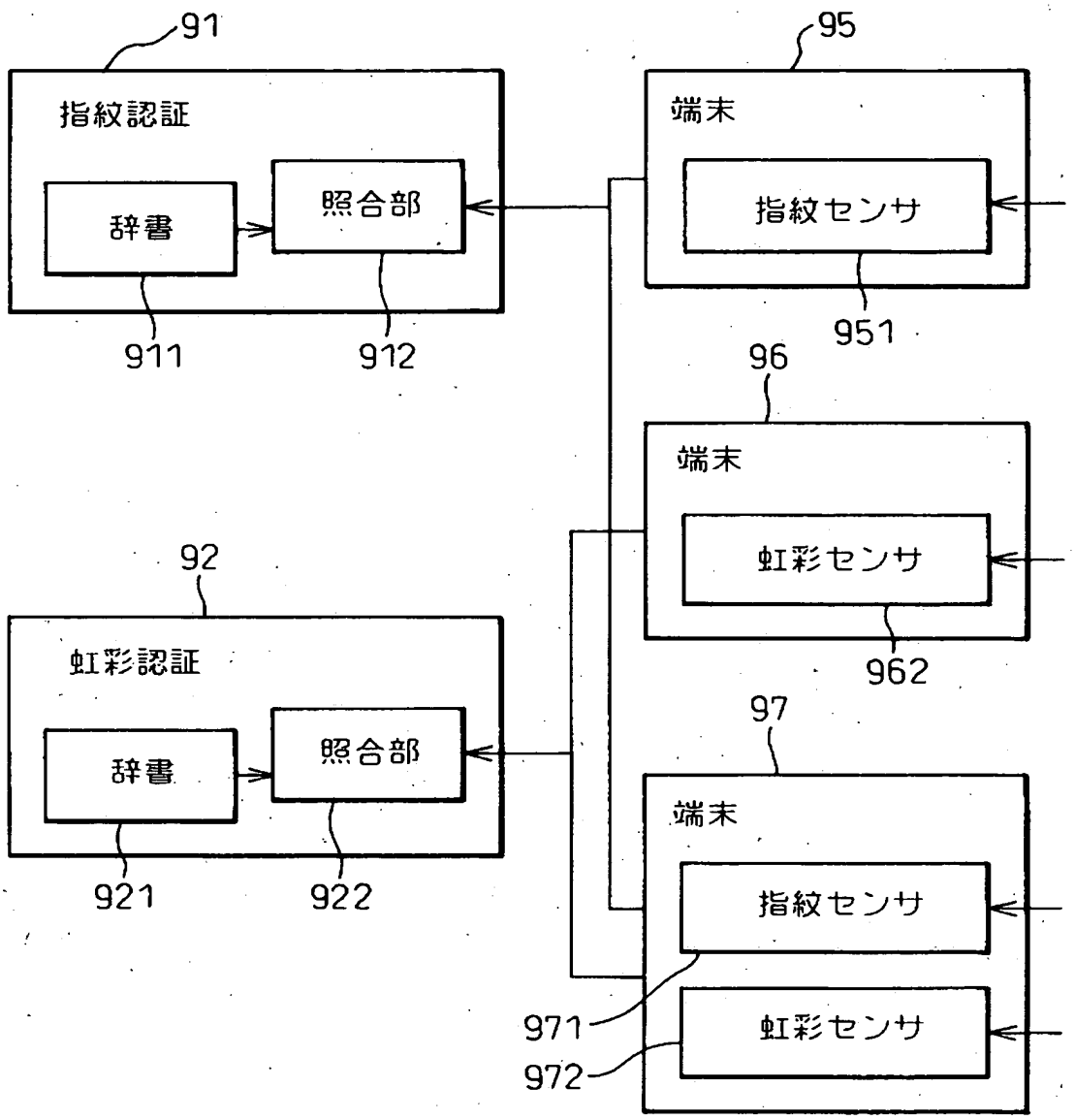
図13


第10実施例
生体情報取得装置
500
センサ
501-n
センサ
501-1
502
暗号化部
(暗号化鍵)
(復号鍵)
503
502
端末
200
生体情報保持部
201
ユーザ
認証装置
100

【図１４】

図 14

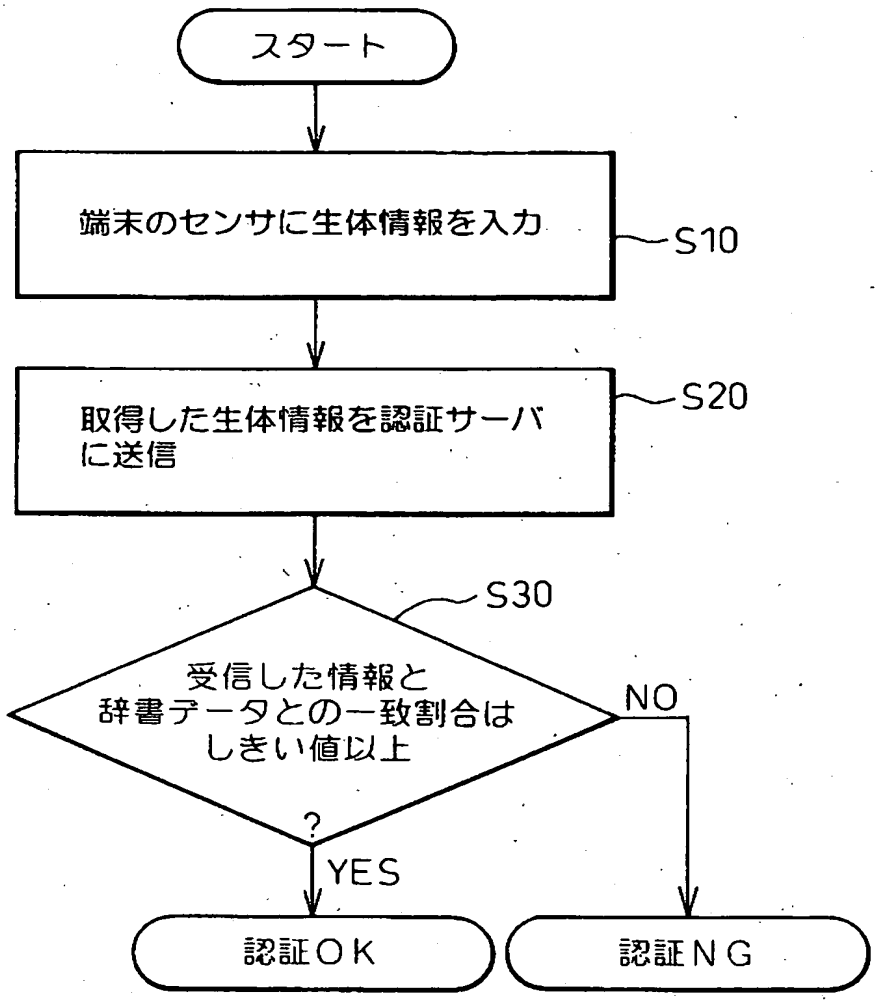
従来の生体情報認証



【図１５】

図 15

従来の生体情報認証フロー



【書類名】　　要約書

【要約】

【課題】　認証手段が相違する各種生体情報認証サーバに対応可能な認証端末及び認証システムを提供する。

【解決手段】　認証端末１０に、本人の各種生体情報を保持する生体情報保持部１と例えば指紋のような生体情報を得るセンサ２とを設け、認証サーバから認証に必要な、例えば虹彩情報のような生体情報を要求された場合、本人の生体情報データ（指紋）をセンサ２に入力して、認証部３で指紋認証を行って本人認証した後、認証サーバが要求する生体情報（虹彩情報）を生体情報保持部１から選択して送信する。

【選択図】　　図１

特願２００３－１７０７２３

# 出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　神奈川県川崎市中原区上小田中１０１５番地
氏　名　　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社